Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Ратушняка Максима Віталійовича

на здобуття ступеня вищої освіти Бакалавра

Система захисту офісу фірми
від витоку інформації технічними каналами зв'язку

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.200113.20.01.16 ПЗ

Виконав студент 4 курсу група КБ-20-1 Максим РАТУШНЯК
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ратушняка Максима Віталійовича

1 Тема роботи Система захисту офісу фірми від витоку інформації технічними каналами зв'язку

Керівник роботи Чешун Віктор Миколайович

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи Створити систему захисту в офісі фірми «SecurLine» від витоку інформації технічними каналами зв'язку

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження захищеності, канали витоку інформації, технічні канали витоку інформації. Існуючі ризики і загрози для системи захисту, заходи захисту від витоку інформації. Дослідження компанії, пасивні заходи захисту офісу, засоби захисту, реалізація захисту і планування, обізнаность персоналу. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Модель порушника. Покімнатні плани контрзаходів

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень	ВИКОНАНО
Ознайомлення з предметною областю	Лютий	ВИКОНАНО
Дослідження існуючих рішень	Лютий	ВИКОНАНО
Постановка задачі	Березень	ВИКОНАНО
Визначення загальних принципів рішення задачі	Березень	ВИКОНАНО
Деталізація принципів рішення задачі	Квітень	ВИКОНАНО
Розробка проєктних рішень	Квітень	ВИКОНАНО
Апробація проєктних рішень	Травень	ВИКОНАНО
Оформлення пояснювальної записки згідно вимог	Травень	ВИКОНАНО
Оформлення графічної частини	Червень	ВИКОНАНО
Захист КР	Червень	ВИКОНАНО

Студент Максим РАТУШНЯК

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту офісу фірми від витоку інформації технічними каналами зв'язку.

Автор роботи: Ратушняк Максим Віталійович

Керівник роботи: к.т.н., доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 67 сторінок, 27 рисунків, 1 додаток, 44 посилання.

Графічна частина: 6 плакатів, 10 презентаційних слайдів.

СИСТЕМА ЗАХИСТУ, ВИТІК ІНФОРМАЦІЇ, ТЕХНІЧНІ КАНАЛИ ЗВ'ЯЗКУ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ЗАКЛАДНІ ПРИСТРОЇ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ.

Метою кваліфікаційної роботи: є розробка ефективної системи захисту офісу компанії від витоку інформації з урахуванням теоретичних основ, аналізу ризиків та загроз, а також специфіки конкретної компанії.

Кваліфікаційна робота присвячена розробці системи захисту офісу компанії від витоку інформації технічними каналами зв'язку. Розглянуто поняття захищеності, каналами витоку інформації, зокрема, технічі. Проаналізовано існуючі ризики та загрози для системи захисту, розглянуто заходи щодо запобігання витоку інформації та використання засобів захисту. Дослідження фокусується на конкретній компанії, де вивчаються її особливості та потреби в захисті від витоку інформації.

Запропоновано пасивні заходи захисту, такі як планування офісу та впровадження засобів захисту. Також було приділено увагу до важливості обізнаності персоналу з питань інформаційної безпеки та запобігання витоку інформації.

12.06.2024 _____

ANNOTATION

Theme of qualification work: A system to protect the company's office from information leakage via technical communication channels.

Author of the work: Maksym Ratushniak Vitaliiovych

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of work: 67 pages, 27 figures, 1 appendices, 44 links.

Graphic part: 6 posters, 10 presentation slides.

PROTECTION SYSTEM, INFORMATION LEAKAGE, TECHNICAL COMMUNICATION CHANNELS, UNAUTHORIZED ACCESS, EMBEDDED DEVICES, TECHNICAL MEANS OF PROTECTION.

The purpose of the qualification work is to develop an effective system for protecting the company's office from information leakage, taking into account the theoretical foundations, risk and threat analysis, as well as the specifics of a particular company.

The qualification work is devoted to the development of a system for protecting a company's office from information leakage through technical communication channels. The concept of security, information leakage channels, in particular, technical ones, are considered. The existing risks and threats to the security system are analyzed, measures to prevent information leakage and the use of security tools are considered. The research focuses on a specific company, where its features and needs for protection against information leakage are studied.

Passive protection measures, such as office layout and implementation of security features, are suggested. Attention was also paid to the importance of staff awareness of information security and information leakage prevention.

12.06.2024 _____

ЗМІСТ

ВСТУП

Сучасний офіс – це складна інформаційна екосистема, в якій циркулюють величезні потоки конфіденційних даних, що становлять комерційну таємницю та інтелектуальну власність компанії. Захист цієї інформації від витоку через технічні канали зв'язку є критично важливим завданням для забезпечення безпеки бізнесу та збереження його конкурентних переваг. Витік даних може мати руйнівні наслідки, включно з фінансовими втратами, втратою довіри клієнтів та репутаційними ризиками.

Технічні канали зв'язку, такі як електромагнітне випромінювання від комп'ютерів, принтерів та інших електронних пристроїв, а також виведення даних через акустичні та віброакустичні перешкоди, створюють потенційні вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до інформації. Крім того, сучасні офісні середовища характеризуються високим ступенем інтегрованості різноманітних технологій, що збільшує кількість потенційних векторів атак та ускладнює процес захисту.

Ця кваліфікаційна робота присвячена розробці системи захисту офісного середовища від витоку інформації через технічні канали зв'язку. У роботі буде проведено ретельний аналіз існуючих загроз, вразливостей та методів захисту, а також запропоновано рішення для підвищення рівня безпеки.

Розроблена система захисту передбачатиме впровадження технічних та організаційних заходів, спрямованих на мінімізацію ризиків витоку інформації. Це включатиме застосування технологій екранування, фільтрації сигналів, а також процедур контролю доступу та моніторингу. Система буде адаптована до специфічних вимог та особливостей роботи конкретної компанії, забезпечуючи максимальний рівень захисту без шкоди для ефективності бізнес-процесів.

Крім того, у роботі буде розглянуто питання підвищення обізнаності персоналу щодо загроз безпеці інформації та методів їх попередження.

Ефективна система захисту вимагає не лише технологічних рішень, а й відповідальної та обізнаної поведінки співробітників у поводженні з конфіденційною інформацією.

Кваліфікаційна робота має на меті створити надійну та комплексну систему захисту, яка забезпечить безпеку офісного середовища від витоку інформації через технічні канали зв'язку, тим самим захищаючи критично важливі дані компанії та підтримуючи її конкурентоспроможність на ринку.

1 ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ, КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

1.1 Дослідження поняття захищеності і системи захисту

Інформація є надзвичайно важливим ресурсом для будь-якої організації чи особи. Вона відіграє ключову роль у прийнятті рішень, здійсненні діяльності та досягненні цілей. Саме тому захист інформації є одним з пріоритетних завдань.

Інформація – це відомості про особи, предмети, факти, події, явища та процеси незалежно від форми їх представлення [1]. Вона може існувати у різноманітних формах: як письмові документи, електронні файли, усні повідомлення, зображення, аудіо- та відеозаписи тощо.

Інформаційна система – це сукупність взаємопов'язаних компонентів, які збирають, обробляють, зберігають і поширюють інформацію для підтримки діяльності організації, управління та прийняття рішень [2].

Інформаційна система складається з таких основних компонентів:

– апаратне забезпечення (комп'ютери, сервери, мережеве обладнання тощо);
– програмне забезпечення (операційні системи, додатки);
– дані та бази даних (структуровані набори даних);
– телекомунікаційні мережі (Інтернет, локальні мережі);
– персонал (користувачі, розробники, аналітики).

Метою інформаційної системи є забезпечити своєчасне надання достовірної інформації для прийняття ефективних рішень і досягнення цілей організації.

Зловмисник – це особа або група осіб, які займаються незаконною діяльністю в Інтернеті або через комп'ютерні системи. Основною метою зловмисника є отримання несанкціонованого доступу до комп'ютерних систем, мереж, даних або інформації з метою їх викрадення, модифікації або знищення.

Технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення конфіденційності, цілісності та доступності інформації за допомогою інженерно-технічних заходів [3].

Система захисту від витоку інформації технічними каналами – це комплекс організаційних і інженерно-технічних заходів, спрямованих на запобігання витоку інформації технічними каналами.

Об'єкт захисту в кібербезпеці – це будь-який компонент інформаційної системи або мережі, який потребує захисту від загроз кібербезпеці [4]. Це може бути:

– інформація;

– системи обробки інформації;

– послуги;

– фізичні об’єкти.

Інформаційна безпека – це захист інформаційних ресурсів та активів організації від різноманітних загроз, спрямованих на порушення їх конфіденційності, цілісності та доступності. Забезпечення інформаційної безпеки має вирішальне значення для захисту бізнесу, репутації та конкурентоспроможності будь-якої організації [5].

Інформаційна безпека організації – це комплексний підхід до захисту конфіденційності, цілісності та доступності інформаційних активів організації, включаючи дані, системи та процеси, від внутрішніх і зовнішніх загроз [6].

Система захисту від витоку інформації технічними каналами – це комплекс організаційних та інженерно-технічних заходів, спрямованих на запобігання витоку інформації технічними каналами.

Аспекти захисту інформації:

– конфіденційність

– цілісність

– доступність.

Конфіденційність означає забезпечення того, щоб інформація залишалася приватною і була доступною лише уповноваженим особам або організаціям. Це означає захист від несанкціонованого розголошення, витоку або доступу до конфіденційних даних [7].

Цілісність – це збереження точності, повноти та узгодженості інформації протягом усього її життєвого циклу. Це включає захист від несанкціонованої модифікації, пошкодження або викривлення даних, що може вплинути на їхню надійність і правильність [8].

Доступність означає забезпечення своєчасного та надійного доступу до інформації та пов'язаних з нею ресурсів для авторизованих користувачів і систем. Це включає захист від блокування, відмови в обслуговуванні або будь-яких інших ситуацій, які можуть перешкоджати доступу до інформації в разі потреби. Доступність також передбачає можливість швидкого відновлення даних у разі їх втрати або пошкодження [9].

Загроза інформаційній безпеці – це сукупність умов і факторів, що створюють ризик порушення інформаційної безпеки [10]. Загрози інформації:

Загрози цілісності:

– знищення;

– модифікація.

Знищення – це навмисне або випадкове видалення, стирання або пошкодження даних, що призводить до втрати цілісності інформації.

Модифікація – це несанкціонована зміна або втручання в дані, що може спотворити зміст інформації та призвести до втрати її цілісності.

Загрози доступності:

– блокування;

– знищення.

Блокування означає перешкоджання авторизованому доступу до інформації, наприклад, через відмову в обслуговуванні або шкідливе програмне забезпечення.

Знищення – це навмисне або випадкове видалення чи пошкодження даних, що робить їх недоступними для авторизованих користувачів.

Загрози конфіденційності:

– несанкціонований доступ;

– витік;

– розголошення.

Несанкціонований доступ (НСД) – це доступ до конфіденційної інформації осіб або організацій, які не мають на це повноважень.

Витік – розголошення конфіденційної інформації внаслідок випадкового або навмисного витоку даних.

Розголошення – навмисне або ненавмисне розкриття конфіденційної інформації особам або організаціям, які не мають права на її отримання.

Ці загрози можуть виникати з різних причин, таких як помилки в системах безпеки, шкідливе програмне забезпечення, людський фактор (навмисні або ненавмисні дії користувачів), фізичні загрози (стихійні лиха, крадіжка обладнання тощо) та інші фактори ризику.

Загрози інформаційній безпеці – це потенційні події або дії, які можуть призвести до порушення конфіденційності, цілісності або доступності інформаційних ресурсів і систем організації [11].

1.2 Канали витоку інформації в системі їх функціонування

Канал зв'язку – це шлях або середовище, через яке сигнали або дані передаються від джерела до одного або декількох приймачів [12].

Дротові канали – сигнал передається через провідник [13], наприклад

– телефонні лінії
– коаксіальні кабелі
– вита пара
– оптоволоконні кабелі.

Бездротові канали (бездротові):

– радіоканали;
– інфрачервоні канали;
– оптичні атмосферні канали;

– акустичні канали.

Радіоканали – сигнал передається у вигляді радіохвиль [14].

Інфрачервоні канали – сигнал передається за допомогою інфрачервоного випромінювання до цілі [15].

Оптичні атмосферні канали – сигнал передається за допомогою оптичного випромінювання в атмосфері [16].

Акустичні канали – сигнал передається у вигляді звукових хвиль[17], наприклад:

– підводні акустичні канали;

– ультразвукові канали.

Електромагнітні канали – сигнал передається за допомогою електромагнітних хвиль, наприклад [18]:

– лінії електропередачі.

Комунікаційна система – це сукупність апаратних, програмних засобів, інформаційних ресурсів та організаційних заходів, призначених для забезпечення обміну інформацією між різними суб'єктами [19].

Комунікаційна система складається з декількох основних компонентів:

– відправник;

– кодування;

– повідомлення;

– канал передачі;

– декодування;

– одержувач;

– зворотній зв'язок;

– шум.

Відправник (джерело) – це людина або пристрій, який генерує повідомлення для передачі [20].

Кодування – процес перетворення ідей або інформації відправника в символи або сигнали, зрозумілі для каналу передачі [21].

Повідомлення – закодована інформація або набір символів, що передається [22].

Канал передачі – засіб або шлях, яким повідомлення надсилається від відправника до одержувача [23].

Декодування – процес інтерпретації отриманих сигналів або символів у форму, яка має сенс для одержувача [24].

Одержувач – особа або пристрій, якому призначене повідомлення і який інтерпретує його зміст.

Зворотний зв'язок – інформація про успішність комунікації, отримана відправником від одержувача [25].

Шум – це будь-який вид перешкод або спотворень, які можуть змінити або погіршити точність передачі інформації.

Ось графічне представлення комунікаційної системи зображено на рисунку 1.1.

Рисунок 1.1 – Графічна схема

Ця схема ілюструє потік інформації від відправника до одержувача, враховуючи можливі перешкоди (шум) і зворотний зв'язок, який забезпечує підтвердження або відповідь на отримане повідомлення.

Офіс компанії – це фізичне місце, де здійснюється управлінська, адміністративна та інша діяльність компанії. Він може включати робочі місця для

співробітників, зони прийому клієнтів і відвідувачів, конференц-зали для зустрічей, а також технічні засоби для зберігання та обробки інформації.

Також зони відпочинку та інші допоміжні приміщення. Офіс фірми слугує центральним пунктом координації бізнес-операцій і комунікацій, сприяючи ефективному функціонуванню організації.

Канали витоку інформації можна розділити на дві основні категорії:

– прямі;

– непрямі.

Прямі канали витоку інформації – канали, через які інформація передається безпосередньо і цілеспрямовано від джерела до зловмисника. Приклади:

– крадіжка документів, комп'ютерів або носіїв інформації;

– навмисне розголошення даних інсайдерами або зрадниками;

– перехоплення незахищених мережевих з'єднань або передач;

– витік через бекдори або шкідливе програмне забезпечення.

Непрямі канали витоку інформації – канали, через які інформація може витекти побічно або ненавмисно, без прямої передачі даних зловмиснику.

Приклади:

– відновлення інформації з викинутого сміття (залишків документів);

– аналіз побічних електромагнітного випромінювання від пристроїв;

– соціальна інженерія для обману працівників і отримання інформації;

– витік через зовнішні сервіси, підрядників або ланцюжки поставок.

Прямі канали зазвичай пов'язані з навмисними діями зловмисників, тоді як непрямі канали можуть виникати через недогляди, помилки або недоліки в системах безпеки.

Атака сторонніми каналами – це тип атаки в інформаційній безпеці, при якій зловмисник намагається отримати конфіденційну інформацію шляхом аналізу фізичних проявів обчислювальних процесів, а не безпосередньо досліджуючи зашифровані дані [26].

1.3 Технічні канали

Технічні канали витоку інформації – це канали, через які може відбуватися несанкціонована передача, витік або розголошення конфіденційної інформації з використанням технічних засобів, пристроїв або систем [27].

Загалом, технічні канали витоку інформації поділяються на наступні:

– акустичні канали;

– віброакустичні канали;

– акустоелектричні канали;

– оптико-електронний.

Акустичні канали витоку інформації – це потенційні шляхи, через які конфіденційна інформація може стати доступною завдяки акустичним хвилям або вібраціям у повітрі [28].

Рисунок 1.2 ілюструє витік інформації з акустичного джерела інформації.

Рисунок 1.2 – Акустичні канали витоку інформації [29]

Ця інформація може випромінюватися з різних джерел, таких як розмови, комп'ютери, принтери або інші електронні пристрої.

Ось деякі приклади акустичних каналів витоку:

– лазівки в конструкціях будівлі;

– прослуховувальні пристрої;

– відбиті/вібраційні сигнали;

– акустична емісія комп'ютерів;

– резонансні ефекти.

Протікання будівельних конструкцій – недостатня звукоізоляція приміщень може призвести до витоку звуку через стіни, вікна або інші отвори.

Пристрої для прослуховування – зловмисники можуть розміщувати приховані мікрофони або пристрої для запису розмов.

Відбиті/вібраційні сигнали – звукові хвилі можуть відбиватися від поверхонь або викликати їхню вібрацію, що дозволяє перехоплювати інформацію.

Акустичні випромінювання від комп'ютерів – комп'ютери та електронні пристрої можуть видавати звукові сигнали, пов'язані з їхньою роботою, які можуть бути використані для витоку даних.

Резонансні ефекти – звукові хвилі можуть бути посилені резонансними ефектами в певних структурах, що збільшує ризик витоку інформації [30].

Віброакустичні канали витоку інформації – це канали, через які можна перехопити конфіденційні дані шляхом вимірювання та аналізу вібрацій і акустичних сигналів, викликаних роботою різних пристроїв і систем. Ось більш детальне визначення:

Віброакустичні канали витоку інформації виникають внаслідок того, що під час роботи різних електронних пристроїв, механізмів і систем генеруються специфічні вібраційні та акустичні сигнали. Ці сигнали можуть містити приховану інформацію про внутрішні процеси в таких системах, наприклад, обробку даних в комп'ютерах або роботу різних механізмів.

Потенційними джерелами віброакустичних сигналів є комп'ютери, принтери, жорсткі диски, кулери охолодження, електродвигуни, механізми друку, а також корпуси та інші конструктивні елементи, які можуть вібрувати.

Віброакустичні канали зображено на рисунку 1.3.

Рисунок 1.3 – Віброакустичні канали витоку інформації [29]

Витік інформації по віброакустичному каналу може відбуватися в результаті:

– прямого запису акустичних сигналів мікрофонами;

– вимірювання вібрацій конструкцій датчиками;

– детектування вібрацій лазерними або радіосистемами.

Безпосередній запис акустичних сигналів за допомогою мікрофонів – цей метод використовується для виявлення та аналізу звукових хвиль, що генеруються вібраціями або коливаннями різних об'єктів.

Вимірювання вібрацій елементів конструкцій за допомогою спеціальних датчиків – в цьому випадку для вимірювання вібрацій використовуються спеціальні датчики, які кріпляться безпосередньо до елементів конструкцій, таких як балки, колони, фундаменти та інші елементи будівель або інженерних споруд.

Використання лазерних або радіосистем для виявлення вібрацій – цей метод заснований на використанні лазерних або радіохвильових систем для безконтактного вимірювання вібрацій об'єктів.

Акустоелектричні канали витоку інформації – це канали, через які може бути перехоплена конфіденційна інформація шляхом вимірювання та аналізу електромагнітних полів та індукованих струмів, що генеруються акустичними коливаннями всередині електронних пристроїв і систем.

Більш детальне визначення:

Під час обробки даних в електронних пристроях, таких як комп'ютери, смартфони, різні мікросхеми та друковані плати, генеруються слабкі акустичні коливання. Ці коливання можуть взаємодіяти з провідниками та напівпровідниковими структурами, генеруючи змінні електромагнітні поля та індуковані струми.

На рисунку 1.4 показано приклад витоку інформації з акустико-електричного джерела інформації.

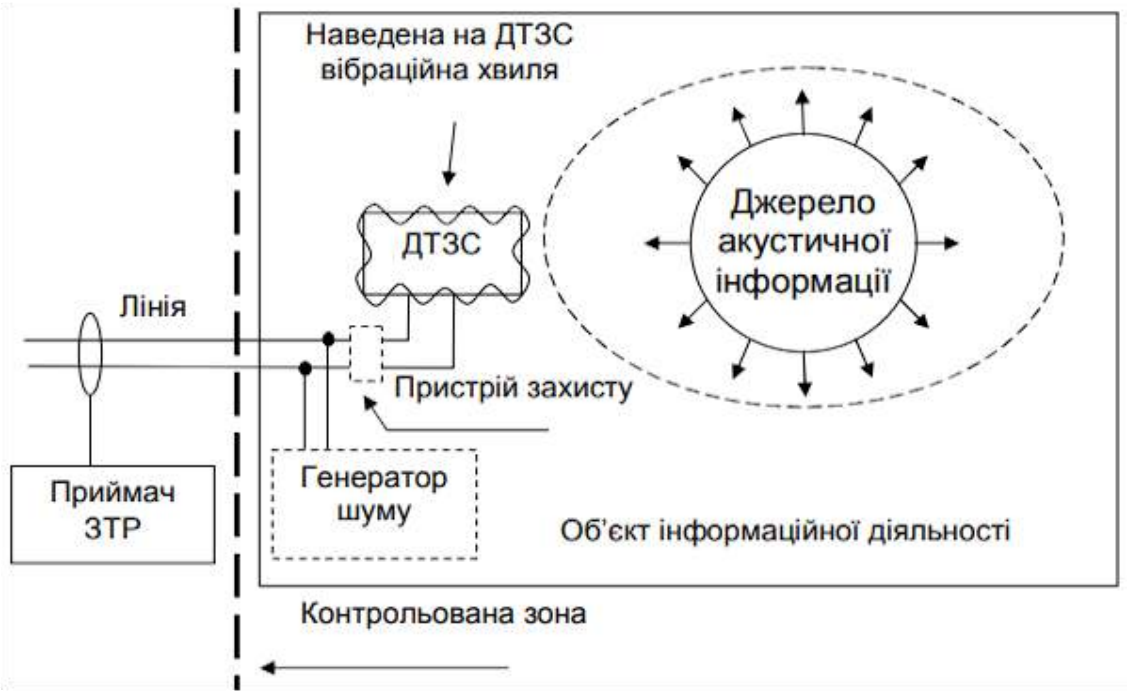


Рисунок 1.4 – Акустоелектричні канали витоку інформації [29]

Ці акустично згенеровані електромагнітні сигнали можуть бути співвіднесені з певною інформацією, що обробляється в пристрої, такою як криптографічні ключі, паролі або інші конфіденційні дані.

Перехоплення інформації через акустоелектричні канали за допомогою:

– вимірювання електромагнітних полів за допомогою спеціальних антен;

– реєстрації індукованих струмів у провідниках;

– підключення до ланцюгів вимірювального пристрою сигналу.

Вимірювання електромагнітних полів навколо пристрою за допомогою спеціальних антен або датчиків.

Реєстрація індукованих струмів у провідниках або лініях передачі даних поблизу пристрою.

Підключення сигналу до ланцюгів вимірювального приладу це процес встановлення електричного з'єднання між вимірювальним приладом і сигналом, що підлягає вимірюванню.

Захист від акустико-електричних каналів включає екранування електромагнітних полів, використання ізольованих провідників, застосування технологій зменшення шуму та спеціальних методів захисту для мінімізації витоку акустично генерованих сигналів.

Оптоелектронний (лазерний) канал витоку інформації – це канал, через який конфіденційні дані можуть бути перехоплені шляхом вимірювання та аналізу вторинного випромінювання від різних електронних пристроїв і систем, таких як монітори, принтери, світлодіоди та інші оптоелектронні компоненти. На рисунку 1.5 показано витік інформації з оптоелектронного каналу.

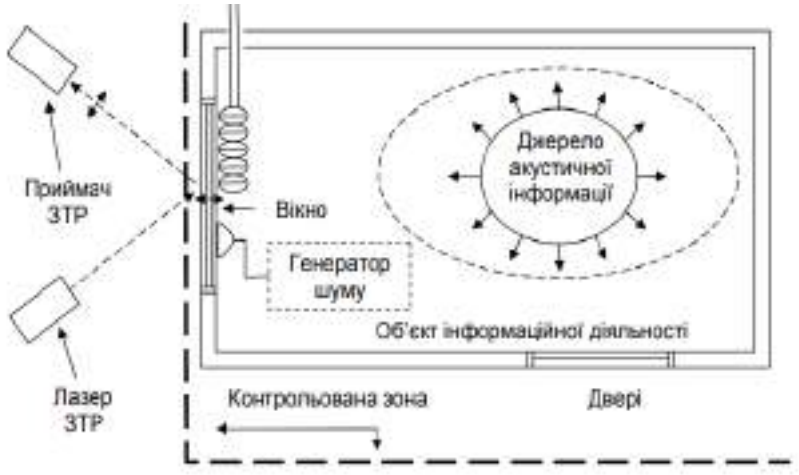


Рисунок 1.5 – Оптико-електронний канал витоку інформації [29]

Більш детальне визначення:

Під час роботи різних електронних пристроїв їхні дисплеї, світлодіоди, лазери та інші оптичні компоненти випромінюють певну кількість світла у видимому та невидимому спектрі.

Це випромінювання може нести приховану інформацію про внутрішні процеси та дані, що обробляються в цих пристроях.

Витік інформації через оптико-електронний канал може відбуватися через

– відбите випромінювання від екранів із залишковим зображенням;

– випромінювання світлодіодів, модульоване внутрішніми сигналами;

– оптичне випромінювання від волоконно-оптичних ліній;

– вторинне випромінювання від взаємодії лазера з поверхнями.

Відбите випромінювання від екранів моніторів, що містять залишкові зображення обробленої інформації.

Випромінювання від світлодіодів та інших оптичних індикаторів, які можуть модулюватися внутрішніми сигналами пристрою.

Оптичне випромінювання від волоконно-оптичних ліній передачі даних.

Вторинне випромінювання внаслідок взаємодії лазерного променя з поверхнями пристроїв.

Параметричні канали витоку інформації – канали, через які може відбуватися витік конфіденційної інформації у вигляді зміни параметрів спільних ресурсів або схем в обчислювальних системах. Більш детальне визначення:

Параметричні канали виникають, коли кілька процесів, додатків або користувачів спільно використовують певні загальні обчислювальні ресурси, такі як процесор, пам'ять, жорсткі диски, шини даних тощо. Коли один процес використовує спільний ресурс, він може змінювати деякі параметри цього ресурсу, такі як затримка доступу, швидкість передачі даних, розмір пам'яті або енергоспоживання.

Ці зміни параметрів можуть бути виявлені іншими процесами, які отримують доступ до того ж ресурсу, і використані для вилучення конфіденційної інформації, наприклад, криптографічних ключів, паролів або інших захищених даних.

Приклади параметричних каналів витоку:

– зміни в затримці доступу до пам'яті через чутливі дані;

– коливання продуктивності через конкуренцію за ресурси;

– зміна часу відгуку через обробку конфіденційної інформації;

– витік даних через енергоспоживання або тепловиділення.

Зміни затримок доступу до спільної пам'яті, які залежать від обробки конфіденційних даних.

Коливання продуктивності системи через конкуренцію за спільні обчислювальні ресурси.

Зміна часу відгуку системи через обробку конфіденційної інформації.

Витік даних через споживання енергії або виділення тепла під час обробки конфіденційних даних.

1.4 Постановка задачі

Для побудови системи захисту від витоку інформації технічним каналами в офісі необхідно краще ознайомитись й дослідити ризики і загрози, що можуть негативно вплинути на функціонування офісу, що буде описано в другому розділі. Також необхідно визначитись з обладнанням для системи захисту і спланувати заходи запобіганню витоку інформації. Вимоги:

Ідентифікація та аналіз потенційних технічних каналів витоку інформації:

– провідникові канали;

– акустичні канали;

– електромагнітні канали;

– оптичні канали.

Впровадження заходів технічного захисту:

– встановлення систем екранування та фільтрації для провідникових каналів;

– використання звукоізолюючих матеріалів та акустичних екранів для акустичних каналів;

– застосування електромагнітних екранів для електромагнітних каналів;

– використання жалюзі, штор або спеціальних плівок для оптичних каналів.

Забезпечення фізичного контролю доступу до приміщень та обладнання:

– встановлення систем контролю доступу;

– обмеження доступу до критичних зон та обладнання;

– моніторинг та реєстрація доступу.

Успішна реалізація цієї системи захисту дозволить мінімізувати ризики витоку конфіденційної інформації через технічні канали зв'язку та забезпечити належний рівень безпеки для діяльності фірми.

2 ІСНУЮЧІ РИЗИКИ І ЗАГРОЗИ ДЛЯ СИСТЕМИ ЗАХИСТУ, ЗАХОДИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ

2.1 Аналіз ризиків і загроз

Проаналізуємо можливі ризики і загрози. Технічні засоби промислового шпигунства – пристрої, обладнання та методи, які використовують зловмисники для несанкціонованого доступу до конфіденційної інформації про науково-технічні чи виробничі процеси в організаціях чи об'єктах [30].

Засоби акустичного контролю – технічні пристрої та системи, що використовуються для виявлення, перехоплення та аналізу акустичних (звукових) сигналів з метою отримання конфіденційної інформації або контролю певних об'єктів [31]. До засобів акустичного контролю відносяться:

Системи прослуховування:

- пристрої для підслуховування (жучки, мікрофони);
- лазерні мікрофони;
- параболічні мікрофони.

Прилади для виявлення акустичної емісії:

- детектори акустичної емісії (для контролю цілісності конструкцій);
- віброакустичні перетворювачі (для моніторингу обладнання).

Системи перехоплення сигналів акустичного наведення:

- прилади для вимірювання акустоелектричних полів;
- перетворювачі акустичного тиску.

Засоби аналізу акустичних сигналів:

- спеціалізовані програмні комплекси;
- системи розпізнавання голосу;
- виділення корисного сигналу з шуму;
- акустичні локаційні пристрої.

Апаратура акустичного моніторингу може використовуватися для прослуховування розмов, збору акустичної інформації про роботу обладнання,

виявлення прихованих порожнин, моніторингу виробничих процесів тощо.

Апаратура віконного спостереження – це технічні засоби та обладнання, що використовуються для перехоплення конфіденційної інформації, яка відображається на моніторах комп'ютерів або інших відео пристроях через їхні вікна. До такого обладнання відносяться:

Відеоспостереження з високою роздільною здатністю:

- телескопічні фотооб'єктиви;
- високочутливі відеокамери;
- інфрачервоні/тепловізійні камери.

Системи лазерної вібродіагностики:

- лазерні віброметри;
- лазерні допплерівські віброметри.

Сканери електромагнітного випромінювання для дисплеїв:

- спеціалізовані антени для перехоплення електромагнітних випромінювання;
- електромагнітні зонди для зчитування залишкових полів.

Оптичні системи для резистивного виявлення зображень:

- високочутливі фотодетектори;
- спеціальні оптичні фільтри та підсилювачі;
- аналітичне програмне забезпечення.

Це обладнання дозволяє зловмисникам перехоплювати конфіденційну інформацію через віконне скло на значній відстані від об'єкта, використовуючи лазерні, оптичні та радіочастотні методи зчитування даних з дисплеїв.

Спеціальна звукозаписувальна апаратура – це технічні засоби, призначені для негласного запису звукових сигналів (розмов, шумів тощо) з метою отримання конфіденційної інформації.

До таких технічних засобів відносяться:

- приховані підслуховуючі пристрої;
- провідні та безпровідні мікрофони;
- мікрофони з цифровим записом;

– мікрофони з функцією передачі даних.

Лазерні мікрофони:

− пристрої для зчитування вібрацій поверхонь за допомогою променя.

Параболічні мікрофони:

− мікрофони з параболічним рефлектором.

Мікрофонні масиви:

− групи мікрофонів для просторової селекції звуків.

Цифрові диктофони:

− портативні пристрої для запису звуку;

− диктофони з функцією приховування/маскування;

− обладнання для обробки та аналізу звукових сигналів;

− спеціалізоване програмне забезпечення;

− системи розпізнавання мови.

Таке обладнання дозволяє негласно записувати розмови на значних відстанях, в приміщеннях, автомобілях та інших місцях, а також аналізувати і витягувати корисні аудіо дані.

Як засоби акустичного контролю і перехоплення конфіденційної інформації можуть використовуватися мікрофони різного призначення і конструкції. Нижче наведені різні типи мікрофонів та їх застосування:

Приховані мікрофони (жучки):

− міні-мікрофони, заховані в різних предметах;

− закладки з мікрофонами і передавачами для передачі звуку на відстань.

Мікрофонні решітки (антенні решітки):

− групи мікрофонів для підсилення та фокусування звуку;

− використовуються для прослуховування на великих відстанях.

Лазерні мікрофони:

– безконтактні пристрої для зчитування вібрацій поверхонь за допомогою променя зчитування;

– дозволяють перехоплювати звуки через вікна, стіни тощо.

Електретні мікрофони:

− компактні, високочутливі мікрофони для прихованого запису.

Динамічні мікрофони:

− використовуються для запису в умовах високого рівня шуму.

Конденсаторні мікрофони:

− мікрофони студійного рівня для запису з високою роздільною здатністю.

Мікрофони з датчиком вібрації:

− прикріплюються до твердих поверхонь, щоб вловлювати звуки за допомогою вібрацій.

Таким чином, мікрофони можуть використовуватися зловмисниками для негласного запису розмов, збору акустичної інформації про приміщення, обладнання тощо.

Підслуховуючі пристрої електромереж – це спеціальні технічні засоби, призначені для перехоплення інформації через електромережі будівель і споруд.

До таких пристроїв відносяться

− мережеві передавачі («черв'яки»);

− мережеві приймачі;

− проникаючі рупори;

− індукційні датчики;

− аналізатори електромагнітних завад.

Мережеві передавачі – це пристрої, які підключаються до електромережі та модулюють аудіо сигнали у високочастотні коливання напруги, що дозволяє перехоплені розмови передавати на відстань через електромережу [32].

Мережеві приймачі – це пристрої для прийому і демодуляції сигналів, що передаються черв'яками [32]. Вони можуть бути розміщені в різних точках електромережі для прослуховування.

Проникаючі гучномовці – це спеціальні мікрофони, призначені для запису звуку від вібрацій в електропроводці. Вони дозволяють перехоплювати розмови через контакт з електрифікованими поверхнями.

Індукційні датчики – це пристрої, які генерують індукційні імпульси в електромережі [33]. Реакцію можна використовувати для виявлення звукових коливань і перехоплення розмов.

Аналізатори електромагнітних завад – використовуються для виявлення та аналізу перехоплених сигналів в електромережі [34].

Такі мережеві пристрої дозволяють зловмисникам отримати доступ до конфіденційної інформації в обхід стін приміщення.

Телефонні ремінці – обмотуються навколо телефонного кабелю для перехоплення сигналу. Дозволяють читати розмови за допомогою індукційного зв'язку.

Телефонні «ретранслятори» – підключаються паралельно до лінії і створюють додаткове відведення сигналу, дублюють розмови для запису.

Високочастотні зонди – підключаються до кабелю для наведення високочастотної напруги. Передають перехоплений сигнал на відстань по повітрю.

Пристрої імітації стільникового радіоканалу – імітують базові станції та підключаються до мобільних пристроїв, перехоплюючи дані, що передаються через імітований канал.

Уловлювачі – перехоплюють і розшифровують дані, що передаються між мобільними телефонами та базовими станціями.

Стільникові шлюзи – отримують доступ до мережі оператора і дозволяють прослуховувати, встановлювати програмне забезпечення для злому трафіку та вилучати дані з мобільних пристроїв.

Для прихованого відеоспостереження і перехоплення візуальної інформації використовуються спеціальні системи спостереження і передачі відеосигналу. До таких систем відносяться:

- приховані відеокамери;
- системи передачі відеосигналу;
- оптичні системи спостереження;
- квадрокоптери та дрони з відеокамерами;
- системи стеження та позиціонування;

− системи для злому та перехоплення цифрових відео потоків;

− обладнання для запису та аналізу відеозаписів.

Приховані камери – це міні-камери, замасковані під побутові предмети (ручки, годинники, прикраси тощо). Бездротові камери з автономним живленням.

Система передачі відеосигналу – бездротові відео передавачі для передачі сигналу на відстань. Кодовані канали та системи стенографічного приховування відео.

Системи оптичного спостереження – телескопічні об'єктиви з великим збільшенням. Інфрачервоні та тепловізійні камери для нічного спостереження [35].

Квадрокоптери та дрони з відеокамерами – безпілотні літальні апарати для аерофотозйомки та спостереження.

Системи відстеження та позиціонування – GPS–трекери для відстеження переміщення об'єктів. Лазерні далекоміри для визначення координат.

Системи для злому і перехоплення цифрових відео потоків – злом і розшифровка закодованих потоків відеоспостереження. Перехоплення та запис веб відео трансляцій.

Обладнання для запису та аналізу відео – сервери зберігання відеоданих, програмне забезпечення для аналізу та розпізнавання зображень.

Такі спеціалізовані системи дозволяють здійснювати прихований візуальний контроль об'єктів, записувати і передавати відеоінформацію на великі відстані.

Для зйомки та отримання конфіденційної візуальної інформації в різних умовах і з різною метою використовуються спеціальні камери. До них відносяться

− камери великої дальності;

− камери для зйомки в темряві;

− високошвидкісні камери;

− приховані камери («шпигунські» камери);

− підводні камери;

− повітряні камери;

− мікроскопічні камери;

− рентгенівські камери.

Далекобійні камери – оснащені потужними телеоб'єктивами з великою фокусною відстанню. Дозволяють знімати віддалені об'єкти з високою деталізацією зображення [35].

Камери нічної зйомки – інфрачервоні та тепловізійні камери, дають можливість вести зйомку знімати в повній темряві.

Швидкісні камери – оснащені швидкісним затвором, призначені для зйомки швидкоплинних процесів і подій [35].

Приховані камери – замасковані під побутові предмети (ручки, окуляри, годинники) [35]. Використовуються для прихованої зйомки.

Повітряні камери – камери, встановлені на літаках, дронах і супутниках. Вони дозволяють робити знімки з повітря та космосу.

Мікроскопічні камери – для фотографування дрібних об'єктів і мікроструктур. Дуже висока роздільна здатність.

Рентгенівські камери – створюють зображення за допомогою рентгенівських променів, що дозволяє «бачити» крізь непрозорі об'єкти.

Такі спеціалізовані камери використовуються в промисловому шпигунстві, технічній розвідці, наукових дослідженнях, а також для незаконного отримання конфіденційної інформації.

Прилади денного спостереження та прилади нічного бачення – це спеціалізоване обладнання, яке використовується для візуального контролю та спостереження за об'єктами в різних умовах освітлення.

Прилади денного спостереження:

- бінокли та монокуляри з великим збільшенням;
- високоякісні фотоапарати та відеокамери з потужними об'єктивами;
- телескопічні об'єктиви з великою фокусною відстанню;
- стабілізовані оптичні прилади для спостереження з рухомих платформ;
- оптичні приціли та прицільні системи з високою роздільною здатністю.

Прилади нічного бачення:

- нічні бінокли з електронно-оптичними перетворювачами;

- прицiли нічного бачення з електронно-оптичними підсилювачами;
- тепловізори для контролю теплового випромінювання;
- прилади нічного бачення на матрицях приладів із зарядовим зв'язком;
- лазерні далекоміри та цілевказівники для визначення відстаней.

Такі спеціалізовані пристрої використовуються у військовій справі, правоохоронних органах, розвідці, спостереженні та мисливстві.

Вони також можуть використовуватися злочинцями для незаконного візуального спостереження та збору конфіденційної інформації.

Спеціальні засоби радіоперехоплення та прийому електромагнітних випромінювань і прицілювання призначені для перехоплення конфіденційної інформації, що передається радіоканалами і міститься в електромагнітному випромінюванні електронних пристроїв [36].

До них відносяться

- сканери радіочастотного спектру
- радіоперехоплювачі
- антени та антенні решітки підвищеної чутливості
- аналізатори сигналів і спектра;
- широкосмугові приймачі
- диференціальні датчики електромагнітного поля;
- електромагнітні зонди.

Сканери радіочастотного спектру – визначають наявність і характеристики радіосигналів у заданому діапазоні частот [37]. Використовуються для виявлення джерел радіосигналів.

Радіо перехоплювачі – приймають, демодулюють і записують радіосигнали різних діапазонів. Дозволяють перехоплювати радіопереговори, дані тощо.

Високочутливі антени та антенні решітки – забезпечують прийом слабких радіосигналів, можуть бути спрямованими або ненаправленими.

Аналізатори сигналів і спектра – аналізують радіочастотні сигнали та їх модуляцію. Використовуються для дешифрування та відновлення даних.

Широкосмугові приймачі – здатні приймати сигнали в широкому діапазоні частот одночасно. Використовуються для перехоплення різнорідних радіосигналів.

Датчики диференціального електромагнітного поля – призначені для виявлення та вимірювання електромагнітних побічних ефектів. Використовуються для збору даних з моніторів, кабелів тощо.

Електромагнітні зонди – дозволяють реєструвати електромагнітні перешкоди від роботи електронних схем [38].

На рисунку 2.1 показано встановлення мікрофону зі звуководом з зовнішню стіну.

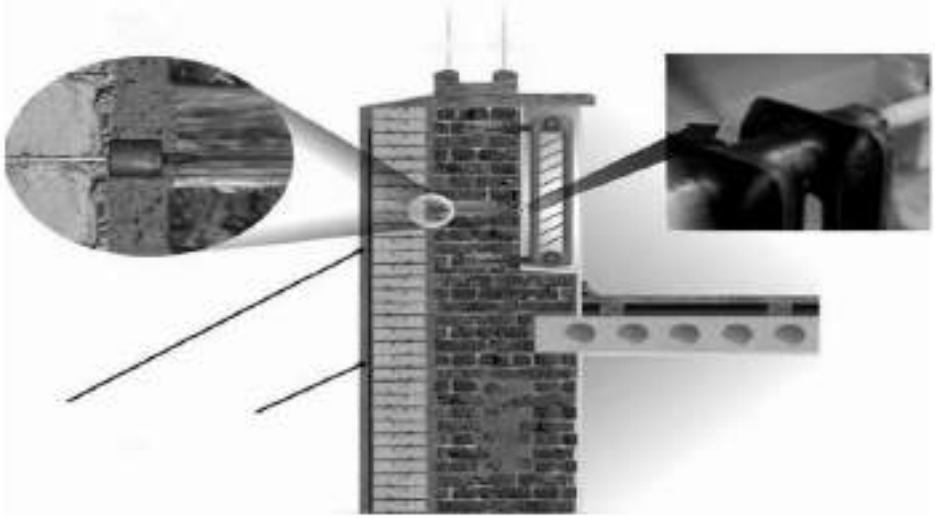


Рисунок 2.1 – Схема встановлення мікрофона зі звуководом в зовнішню стіну [39]

Технічні засоби збору інформації – це пристрої, призначені для негласного отримання або запису конфіденційної інформації [40]. Ці засоби можуть використовуватися як в законних цілях (наприклад, правоохоронними органами), так і з протиправними намірами.

Встановлення інформаційного обладнання в захисних конструкціях під час будівництва та ремонту. Технічні засоби зняття інформації можуть бути впроваджені «противником» в захисні конструкції приміщень під час проведення будівельних, ремонтних та реконструкційних робіт різними способами. Одним із способів є вбудовування прихованих камер і мікрофонів безпосередньо в стіни,

стелю та підлогу, де вони можуть бути замасковані під вентиляційні отвори, освітлювальні прилади або інші елементи інтер'єру.

Крім того, противник може використовувати спеціальні будівельні матеріали, такі як цегла або бетонні блоки, з вбудованим технічним обладнанням, наприклад, мікрофонами або датчиками руху.

Обладнання може бути приховане під час оздоблювальних робіт, наприклад, під штукатуркою, фарбою або підлоговим покриттям, як показано на рисунку 2.2.

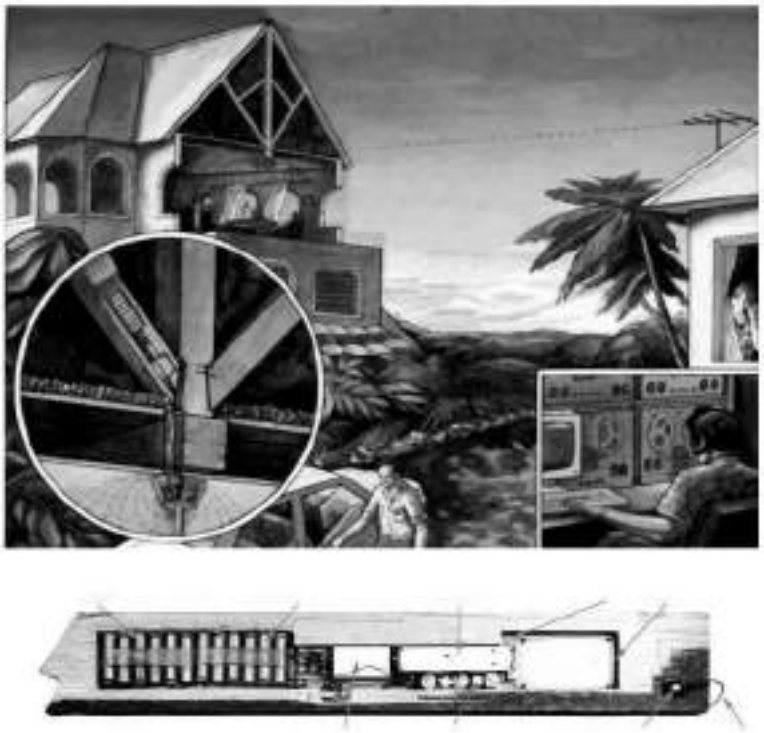


Рисунок 2.2 – Розміщення радіозакладки, закамуфльовану під дерев’яний брусок [39]

Всі ці методи вимагають ретельного планування, використання спеціалізованого обладнання і можуть бути реалізовані тільки під час активних будівельних робіт, щоб забезпечити непомітність і максимальну інтеграцію в конструкцію будівлі.

Технічні засоби зняття інформації можуть бути реалізовані шляхом вбудовування їх у предмети меблів, інші предмети інтер'єру та побуту, а також різні технічні засоби як загального призначення, так і обробки інформації.

Наприклад, невеликі камери та мікрофони можна вбудувати в меблі, такі як шафи, столи, стільці або навіть лампи. На рисунку 2.3 показано, як встановити мережеву закладку в розетку.

Рисунок 2.3 – Технік встановлює мережеву закладку [39]

Приховане обладнання може бути замасковане під декоративні елементи, такі як картини, статуетки або різні предмети побуту.

Загалом, будь-який предмет інтер'єру, побутовий прилад або електронний пристрій потенційно може містити приховане обладнання для зняття інформації, встановлене з метою несанкціонованого доступу до конфіденційних даних.

Також технічні засоби зняття інформації можуть бути впроваджені шляхом встановлення їх у побутові предмети, які даруються в якості подарунків, а в подальшому можуть бути використані для прикрашання інтер'єру офісних приміщень.

«Противник» може заховати міні-камери, мікрофони або інші записуючі пристрої у, здавалося б, звичайних предметах, таких як квіткові композиції, картини, статуетки, канцелярське приладдя або навіть іграшки. Ці предмети потім можуть бути подаровані як безневинний сувенір або подарунок на згадку.

Опинившись в офісі, вони можуть бути використані для прикраси інтер'єру та отримання доступу до конфіденційної інформації.

Наприклад, картину з вбудованою камерою можна розмістити в кабінеті керівника, а статуетку з мікрофоном – у переговорній кімнаті.

Предмети побуту можуть викликати менше підозр, ніж відверто технічні пристрої, і тому є ідеальним прихованим каналом для збору інформації. Наприклад, виявлення радіо закладок у журнальному столику, як показано на рисунку 2.4.

Рисунок 2.4 – Журнальний столик, обладнаний радіо закладками, закамуфльовані під дерев’яний брусок [39]

Противник може заохочувати передачу таких “подарунків”, вдаючи доброзичливість, пропонуючи престижні або дорогі подарунки під виглядом налагодження стосунків.

Прикрашаючи інтер'єр офісних приміщень предметами з вбудованими записуючими пристроями, противник отримує доступ до конфіденційних даних і розмов, що відбуваються в цих приміщеннях. Цей підступний спосіб встановлення пристроїв для збору даних може бути важко виявити.

Також під час обслуговування інженерних мереж і систем у будівлі. ворог може скористатися доступом, наданим ремонтним службам, для проведення профілактичних робіт на комунікаціях, електромережах, системах вентиляції та опалення.

Під час таких профілактичних робіт підрядники, які можуть бути навіть працівниками легальних ремонтних служб, мають вільний доступ до різних приміщень і технічних шахт, а також ідеальні можливості для приховування обладнання для збору інформації.

Наприклад, під час ремонту вентиляційної системи компактні камери та мікрофони можна вмонтувати у вентиляційні решітки або шахти, що забезпечить широкий огляд та якісний запис звуку. При обслуговуванні електричних мереж пристрої можна заховати в корпусах електричних щитків, розеток або навіть лампочок. При ремонті систем опалення та водопостачання жучки можуть бути вмонтовані в елементи трубопроводів або радіаторів. Використання офіційних ремонтних служб підвищує довіру до операції та зменшує підозри.

«Ворог» може проникнути в ці сервіси безпосередньо або схилити їхніх співробітників до співпраці шляхом підкупу, шантажу тощо. Після успішної операції зі встановлення обладнання для збору інформації під виглядом профілактичного ремонту противник отримує приховані канали для постійного спостереження та збору даних про конфіденційну діяльність об'єкта.

2.2 Заходи запобіганню витоку інформації

Для перехоплення мовної інформації існують автономні пристрої, що поєднують в собі мікрофони і передавачі, так звані закладні пристрої (ЗП).

Перехоплена «жучком» мовна інформація може передаватися різними каналами: радіоканалом, мережею електроживлення, оптичним каналом, з'єднувальними лініями дротового телефонного зв'язку, сторонніми провідниками, інженерними комунікаціями в ультразвуковому діапазоні частот, а також по

телефонній лінії шляхом дзвінка зовнішньому абоненту.

Інформація, що передається за допомогою прослуховування, зазвичай приймається спеціальними приймальними пристроями, що працюють у відповідному діапазоні хвиль, але в деяких випадках, наприклад, при передачі по телефонній лінії, прийом може здійснюватися за допомогою звичайного телефону.

Використання портативних диктофонів і записуючих пристроїв зазвичай вимагає проникнення в контрольоване середовище, але в деяких ситуаціях, наприклад, при використанні стетоскопів, проникнення не є обов'язковим. Якщо проникнення в контрольоване приміщення або зону неможливо, для перехоплення мовної інформації використовуються спрямовані мікрофони.

Перш за все, необхідно вжити заходів щодо підвищення звукоізоляції приміщень об'єкта інформаційної діяльності ОІД.

Приміщення, де планується створення ОІД, повинно мати подвійні вхідні двері з тамбуром між ними, який обладнується гумовими ущільнювачами по периметру дверей, звукопоглинальними матеріалами на поверхнях і порогами на підлозі. Глибина тамбура впливає на рівень звукоізоляції – чим більша глибина, тим краще. За наявності додаткового (аварійного) виходу з об'єкта через приміщення, до яких можуть потрапити сторонні особи, конструкція цих дверей повинна бути аналогічною до основних дверей.

Стіни та перегородки повинні бути виконані з бетону або залізобетону товщиною не менше 80 мм або цегли товщиною 120 мм із застосуванням звукопоглинальних матеріалів. Для кращої звукоізоляції необхідно використовувати багатошарові конструкції стін зі звукопоглинальними матеріалами всередині, але без металевих елементів.

Стіни надійно з'єднуються з міжповерховими перекриттями. Під підвісною стелею або підлогою об'єкт не може мати спільний простір з іншими приміщеннями.

Міжповерхові перекриття не повинні мати отворів з боку Оді. Якщо такі є, їх слід заповнити розчином на всю глибину.

Стеля, крім декору, повинна підвищувати звукоізоляцію приміщення.

Варіант – підвісна стеля на еластичних підвісах зі звукопоглинальних плит, без закритих порожнин, які ускладнюють огляд простору під/над нею. Приклад звукоізоляційної стелі зображено на рисунку 2.5.

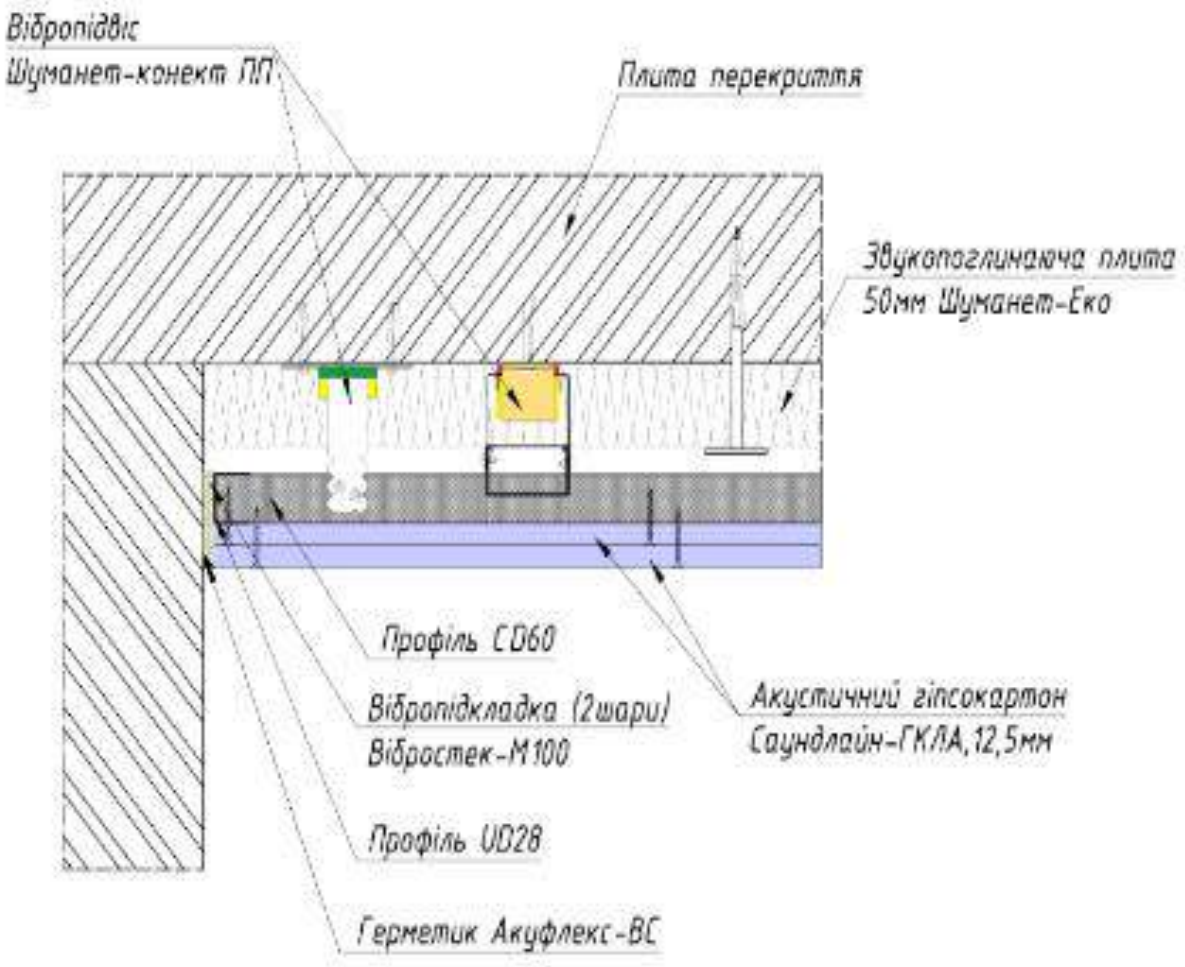


Рисунок 2.5 – Каркасна звукоізоляційна стеля [41]

Підлогу бажано зробити багатошаровою «плаваючою» конструкцією (наприклад, паркет, ламінат) зі звукопоглинальним матеріалом всередині. Плінтуси мають еластичні краї та канали для кабелів.

Приклад плаваючої підлоги можна побачити на рисунку 2.6.

У приміщенні використовуються вікна з підвищеною звукоізоляцією: металопластикові або дерев'яні з трикамерним склопакетом. Різниця між звичайним склопакетом і звукоізоляційним показана на рисунку 2.7.

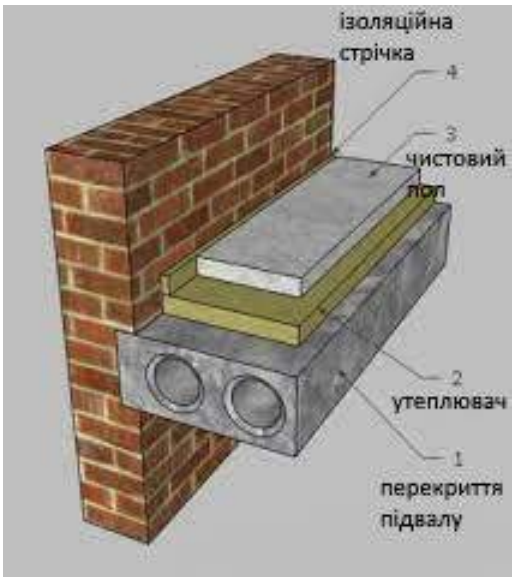


Рисунок 2.6 – Будова плаваючого полу [42]

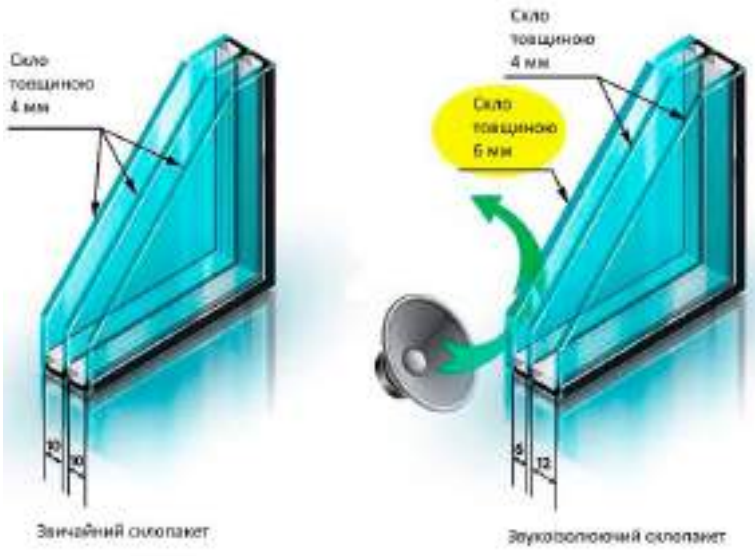


Рисунок 2.7 – Різниця між склопакетами

Фурнітура забезпечує щільне прилягання рухомих елементів протягом щонайменше 2 років. Після завершення ремонтних робіт вікна обладнуються засобами (штори, жалюзі), які унеможливлюють перегляд приміщення ззовні, незалежно від поверху.

2.3 Висновки

В даному розділі ми проаналізували можливі ризики і загрози для системи захисту інформації, зокрема засоби акустичного контролю, апаратуру віконного спостереження, спеціальну звуко записуючу апаратуру, підслуховуючі пристрої електромереж, пристрої негласного зйому візуальної інформації та технічні засоби збору інформації. Розглянули способи впровадження технічних засобів зняття інформації в захисні конструкції під час будівництва, ремонту, через оздоблення інтер'єру та під час обслуговування інженерних мереж і систем.

Розроблено заходи щодо запобігання витоку мовної інформації. Запропоновано підвищити звукоізоляцію приміщень об'єкта інформаційної діяльності шляхом використання спеціальних дверей з тамбуром, звукопоглинальних матеріалів для стін і перегородок, підвісних стель, багатошарових плаваючих підлог та вікон з підвищеною звукоізоляцією.

3 ДОСЛІДЖЕННЯ КОМПАНІЇ, ПАСИВНІ ЗАХОДИ ЗАХИСТУ ОФІСУ, ЗАСОБИ ЗАХИСТУ, РЕАЛІЗАЦІЯ ЗАХИСТУ І ПЛАНУВАННЯ, ОБІЗНАНОСТЬ ПЕРСОНАЛУ

3.1 Дослідження компанії

Назва компанії: «SecurLine». Сфера діяльності компанії це створення систем захисту від витоку інформації технічними каналами зв'язку для державних інформаційних об'єктів ОІД.

Опис послуг: «SecurLine» спеціалізується на розробці та впровадженні комплексних рішень для забезпечення захисту інформації від витоку технічними каналами зв'язку. Послуги включають в себе

– захист від витоку акустичної інформації;

– захист інформації каналами передачі даних;

– технічний захист від електромагнітних випромінювань.

Проектування та монтаж систем захисту від витоку акустичної інформації з використанням звукоізоляції, екранування та спеціалізованого обладнання.

Захист інформації від витоку каналами передачі даних за допомогою криптографічного захисту, встановлення міжмережевих екранів, систем виявлення та попередження вторгнень.

Розробка та впровадження технічних засобів захисту від витоку інформації за рахунок електромагнітних випромінювань та наведень. Клієнти:

– державні установи та організації;

– підприємства оборонно-промислового комплексу;

– комерційні структури, що працюють з конфіденційною інформацією.

Проведення спеціальних обстежень та сертифікаційних випробувань на відповідність вимогам щодо захисту державної таємниці.

Обробка інформації: SecureLine виконує роботи із захисту інформації, що становить державну таємницю зі ступенем секретності «Цілком таємно» на об'єктах другої та третьої категорій відповідно.

3.2 Пасивні заходи захисту

При будівництві офісу фірми були дотримані всі необхідні вимоги та рекомендації для забезпечення належного рівня безпеки та конфіденційності в критично важливих зонах. Зокрема:

- подвійні двері з тамбуром;
- цегляні стіни зі звукоізоляцією;
- підвісна звукопоглинальна стеля;
- багатошарова «плаваюча» підлога;
- звукоізоляційні склопакети;
- жалюзі, що обмежують видимість вікон.

В офісі вхід і кімнати, де це було необхідно, були обладнані подвійними дверима з ущільнювачем і тамбуром між ними. Стіни тамбура облицьовані звукопоглинальними матеріалами, а на підлозі встановлені пороги для поліпшення звукоізоляції.

Стіни та перегородки в приміщенні та кабінеті керівництва виконані з цегляної кладки відповідної товщини та оздоблені звукоізоляційними декоративними покриттями багатошарової конструкції без використання металевих елементів.

Стелі в цих приміщеннях виконані у вигляді підвісної конструкції зі звукопоглинальних плит без закритих порожнин.

Підлоги багатошарові, зі звукоізоляційним шаром всередині, змонтовані за принципом «плаваючої підлоги». Плінтуси мають еластичні краї та кабельні канали.

Вікна – металопластикові двокамерні склопакети з підвищеною звукоізоляцією.

Таким чином, при проектуванні та будівництві офісу були використані новітні технології та матеріали для створення максимально безпечного середовища в критичних зонах відповідно до кращих світових практик.

Вікна офісу обладнані пристроями, які не дозволяють переглядати приміщення ззовні, незалежно від наявності будівель, розташованих навпроти.

3.3 Застосування засобів захисту

Віброакустичний захист – це комплекс технологій, матеріалів і конструкцій, призначених для зниження рівня шуму і вібрації в приміщеннях і спорудах [43]. Вони використовуються для запобігання поширенню звукових і вібраційних хвиль, які можуть негативно впливати на здоров'я людей або точність роботи обладнання.

Обладнання було обрано з сайту ТЗІ, тому зображення і технічні характеристики взяті з нього ж сайту.

Вібровипромінювач ВІ-4 – це спеціально розроблений пристрій, який перетворює електричні сигнали на механічні коливання, створюючи вібрацію. Цей тип вібровипромінювача призначений для використання в системах технічного захисту інформації з метою запобігання витоку даних через віброакустичні канали [44]. Завдяки унікальній конструкції та використанню магнітоелектричних матеріалів, ВІ-4 забезпечує високий рівень вібрації при зниженому рівні паразитних акустичних шумів.

Ось детальні характеристики цього пристрою:

− максимальна потужність: 2 Вт, що забезпечує достатню інтенсивність вібрації для ефективної роботи системи захисту;

− середній рівень звуку на відстані 1 м: 40 дБА, що є відносно низьким рівнем і мінімізує ризик виявлення системи захисту;

− діапазон робочих температур: від 30 до 90°С, що дозволяє використовувати пристрій в різних умовах навколишнього середовища;

− гарантійний термін експлуатації: 8 років, що свідчить про високу надійність і тривалий строк служби;

− розміри корпусу: діаметр 60 мм, висота 22 мм, що робить пристрій компактним і зручним для встановлення;

− кріплення: різьба М8х8, що забезпечує надійне з'єднання з поверхнею;

− маса: 300 г, що є оптимальною для забезпечення необхідної вібрації та зручності монтажу.

Його зображення на рисунку 3.1:

Рисунок 3.1 – Вібровипромінювач ВІ-4 [44]

Вібровипромінювач ВІ-3 – це пристрій, який використовує магнітоелектричні технології для генерування вібрацій із зниженим рівнем паразитних акустичних шумів [44]. Він призначений для систем технічного захисту інформації від витоку через віброакустичні канали. Завдяки своїй конструкції, ВІ-3 забезпечує надійний захист від несанкціонованого доступу до даних.

Його основні характеристики:

− максимальна розсіювана потужність: 1 Вт, що дозволяє ефективно створювати необхідні вібрації;

− середній рівень звуку на відстані 1 м: 40 дБА, що є досить низьким рівнем, який важко виявити;

− діапазон робочих температур: від -10°С до +60°С, що забезпечує стабільну роботу в різних кліматичних умовах;

− середнє напрацювання: 50000 годин, що свідчить про високу надійність і тривалий термін служби;

− гарантійний термін експлуатації: 8 років, що дає впевненість у якості;

− розміри корпусу: діаметр 47,5 мм, висота 16,5 мм, що робить пристрій компактним і зручним для встановлення;

− кріплення: різьба М5х5,5, що забезпечує кріплення до монтажної поверхні;

− маса: 160 г, що є оптимальною для забезпечення необхідної вібрації та зручності монтажу;

Його зображення на рисунку 3.2:

Рисунок 3.2 – Вібровипромінювач ВІ-3 [44]

Генератор шумових сигналів «МАРС-ТЗО-4-2» – це спеціалізований пристрій, призначений для активного захисту мовної інформації від витоку через акустичні та віброакустичні канали [44]. Він використовується на об'єктах інформаційної діяльності другої та третьої категорії, де обробляється інформація, що становить державну таємницю з відповідним ступенем секретності.

Пристрій генерує два незалежні шумові сигнали, які передаються через акустичні колонки та вібровипромінювачі для маскування потенційних витоків інформації.

Його зображення на рисунку 3.3:

Рисунок 3.3 – Генератор шумових сигналів МАРС-ТЗО-4-2 [44]

Ось детальні характеристики генератора шумових сигналів «МАРС-ТЗО-4-2»:

− діапазон частот шумового сигналу: від 180 Гц до 5600 Гц, що забезпечує широкий спектр частот для ефективного маскування;

− ефективне значення вихідної напруги кожного каналу на опорі навантаження 4 Ом: не менше 3,5 В, що забезпечує достатню потужність для акустичних колонок та вібровипромінювачів;

− віброприскорення, що передається від вібровипромінювача ВІ-4 на ізольовану масу 10 кг в усій смузі шумового сигналу: не менше 50 дБ, що забезпечує потужну вібрацію для захисту від віброакустичних витоків;

− звуковий тиск, що створюється колонками акустичними захищеними «МАРС-АКЗ» у вільному полі на відстані 1 м в діапазоні робочих частот: не менше 80 дБ, що забезпечує потужний звуковий сигнал для маскування акустичних витоків;

− діапазон регулювання рівнів шумових сигналів на виходах: не менше 20 дБ, що дозволяє налаштувати оптимальний рівень шумових сигналів;

− режим експлуатації: безперервний протягом 24 годин, що забезпечує постійний захист інформації;

− гарантійний строк експлуатації: 2 роки з дати придбання, що підтверджує якість та надійність пристрою;

− строк служби: 6 років, що забезпечує тривалий термін використання;

− час наробітку на відмову: не менше 10 000 годин, що свідчить про високу надійність пристрою;

− споживана потужність: не більше 40 Вт, що робить пристрій енергоефективним і зручним в різних умовах;

− напруга живлення: від 100 В до 240 В частотою 50, 60 Гц, що забезпечує сумісність з різними джерелами живлення;

− габаритні розміри: не більше 225 мм х 142 мм х 48 мм, що робить пристрій компактним і зручним для встановлення;

− маса: не більше 1,5 кг, що забезпечує портативність.

Мережевий розв'язуючий пристрій «ПМР» є спеціалізованим обладнанням, яке забезпечує гальванічну ізоляцію апаратури, розташованої в захищеному приміщенні, від промислової мережі [44]. Цей пристрій призначений для попередження витоку інформації через канали, пов'язані з електромережею.

Мережевий розв'язуючий пристрій «ПМР» зображено на рисунку 3.4.

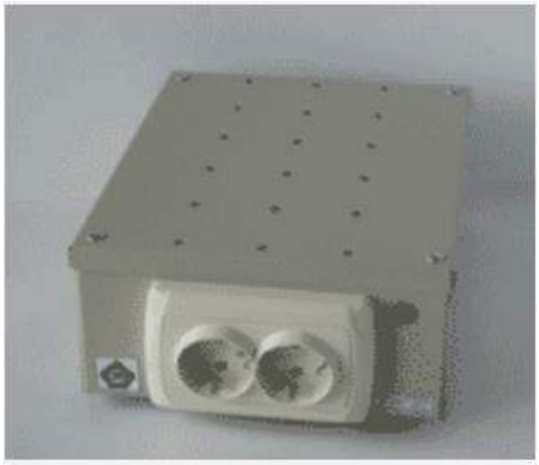


Рисунок 3.4 – Мережевий розв'язуючий пристрій «ПМР» [44]

Ось детальні характеристики мережевого розв'язуючого пристрою «ПМР»:

− номінальна вихідна потужність: не менше 700 (100>0, 1500) Вт, що забезпечує достатню потужність для живлення апаратури в приміщенні;

− напруга живлення: 220 В, що відповідає стандартній напрузі;

− частота живильної мережі: 50 (60) Гц, що дозволяє використовувати пристрій у мережах з різними частотами;

− габаритні розміри: не більше 280 мм х 200 мм х 120 мм, що робить пристрій компактним і зручним для встановлення;

− маса: не більше 15 кг, що забезпечує портативність.

Дротовий датчик руху та розбиття скла Ajax CombiProtect Fibra – це універсальний пристрій безпеки, який поєднує функції виявлення руху та розбиття скла для приміщень. Він має низку особливостей та характеристик, що забезпечують ефективну роботу та запобігання хибним спрацьовуванням. Ось детальний опис його можливостей:

Виявлення руху:

- чутливий елемент: 1 х ІЧ-сенсор;
- дальність виявлення руху до 12 метрів при встановленні на висоті 2,4 ме;
- кути виявлення руху: горизонтальний – 88,5°, вертикальний – 80°;
- напрямок огляду лінзи датчика повинен бути перпендикулярним;
- чутливість: 3 рівні, які можна регулювати в застосунку Ajax;
- імунітет до тварин вагою до 20 кг і зростом до 50 см;
- захист від хибних спрацьовувань SmartDetect;
- температурна компенсація: –10°C до +40°C .

Виявлення розбиття скла:

- чутливий елемент: 1 х електретний мікрофон;
- дальність виявлення розбиття скла до 9 метрів;
- кути виявлення розбиття скла: горизонтальний – 180°;
- чутливість: 3 рівні, які можна регулювати в застосунку Ajax;
- захист від хибних спрацьовувань DualTone;
- програмний алгоритм двофакторної верифікації розбиття скла.

Його зображено на рисунку 3.5:

Рисунок 3.5 – Датчик руху

Магнітоконтактний датчик Ajax DoorProtect Fibra (рисунок 3.6) є провідним шинним датчиком відкриття дверей та вікон, який призначений для використання в охоронній сигналізації Ajax. Він також підтримує підключення додаткового стороннього дротового NC-датчика.

Рисунок 3.6 – Датчик відкриття/закриття дверей

Ось детальні технічні характеристики цього пристрою:

- тип датчика: дротовий шинний датчик відкриття;
- спосіб встановлення: усередині приміщень;
- чутливий елемент: геркон;
- поріг спрацьовування (чутливість датчика на відстані): 1-2 см (малий та великий магніти);
- сумісність: Hub Hybrid (2G), Hub Hybrid (4G);

- надсилання сигналу тривоги: 0,15 секунди;
- протокол: Fibra;
- дальність провідного зв'язку з централлю: до 2000 м (U/UTP cat.5);
- період опитування датчика: 12-300 секунд;
- ресурс роботи: 2 000 000 відкриттів;
- варіанти підключення зовнішнього датчика: NC датчик будь-якого типу;
- тампер (захист від розкриття корпусу): присутній;
- живлення: 24 В;
- клас захисту: IP50;
- іапазон робочих температур: від -10°C до +40°C;
- допустима вологість: до 75%;
- габарити: 90,5 х 21 х 18,5 мм;
- вага: 54 г.

Контролер доступу – це спеціалізований пристрій, який забезпечує контрольований доступ до певних ресурсів, приміщень або інформаційних систем. Він виконує роль своєрідного «воротаря», дозволяючи або блокуючи доступ на основі певних правил та ідентифікаторів.

Контролери доступу широко використовуються в системах безпеки для захисту фізичних та інформаційних активів від несанкціонованого вторгнення зловмисників.

Для системи ми обрали біометричний контролер доступу ZK Software MA300. Цей пристрій поєднує надійні технології ідентифікації та різноманітні функції для забезпечення ефективного контролю доступу.

Зображення контролера доступу ZK Software MA300 на рисунку 3.7.

Рисунок 3.7 – Біометричний контролер доступу

Ось детальні технічні характеристики ZK Software MA300:

– тип пристрою: термінал контролю доступу;
– тип контролера: мережевий та автономний режими роботи;
– методи ідентифікації: безконтактні картки та відбитки пальців;
– сенсор відбитків пальців: високоякісний оптичний сенсор;
– вбудований зчитувач карт: підтримує картки стандарту EM-Marine 125 кГц;
– інтерфейси: Wiegand, RS232, RS485, Ethernet, USB для зв'язку та інтеграції;
– пам'ять для відбитків пальців: до 1500 шаблонів;
– пам'ять для RFID карт: до 10000 карток;
– журнал подій: зберігає до 100000 записів;
– програмне забезпечення: ZKAccess 3.5 для керування та налаштувань;
– додаткові функції: облік робочого часу персоналу;
– живлення: 12В постійного струму;
– ступінь захисту корпусу: IP65 (захист від пилу та бризок води);
– діапазон робочих температур: від –10°C до +60°C;
– розміри: 148 x 73 x 34,5 мм (компактний дизайн).

3.4 Планування офісу і реалізація заходів захисту

Для кращого розуміння з чим ми маємо справу потрібно створити план офісу. Зображення плану офісу компанії можуть бути важливими з декількох причин:

- планування робочого простору;
- організація руху;
- розташування допоміжних приміщень;
- аварійні виходи;
- система безпеки.

Планування розміщення обладнання та робочих місць. План офісу дозволяє ефективно розподілити простір і розмістити меблі, комп'ютери, принтери та іншу необхідну техніку відповідно до ваших потреб.

Організація потоків руху. План офісу допомагає візуалізувати маршрути руху співробітників, відвідувачів та логістичні маршрути доставки документів, щоб оптимізувати трафік.

Розташування допоміжних приміщень. На плані офісу показано розташування переговорних кімнат, кімнат відпочинку, серверних тощо для зручного доступу до них.

Аварійні виходи та плани евакуації. План офісу важливий для розробки чітких інструкцій евакуації в разі надзвичайної ситуації.

Системи безпеки. План дозволяє чітко розмістити системи контролю доступу, пожежні системи тощо.

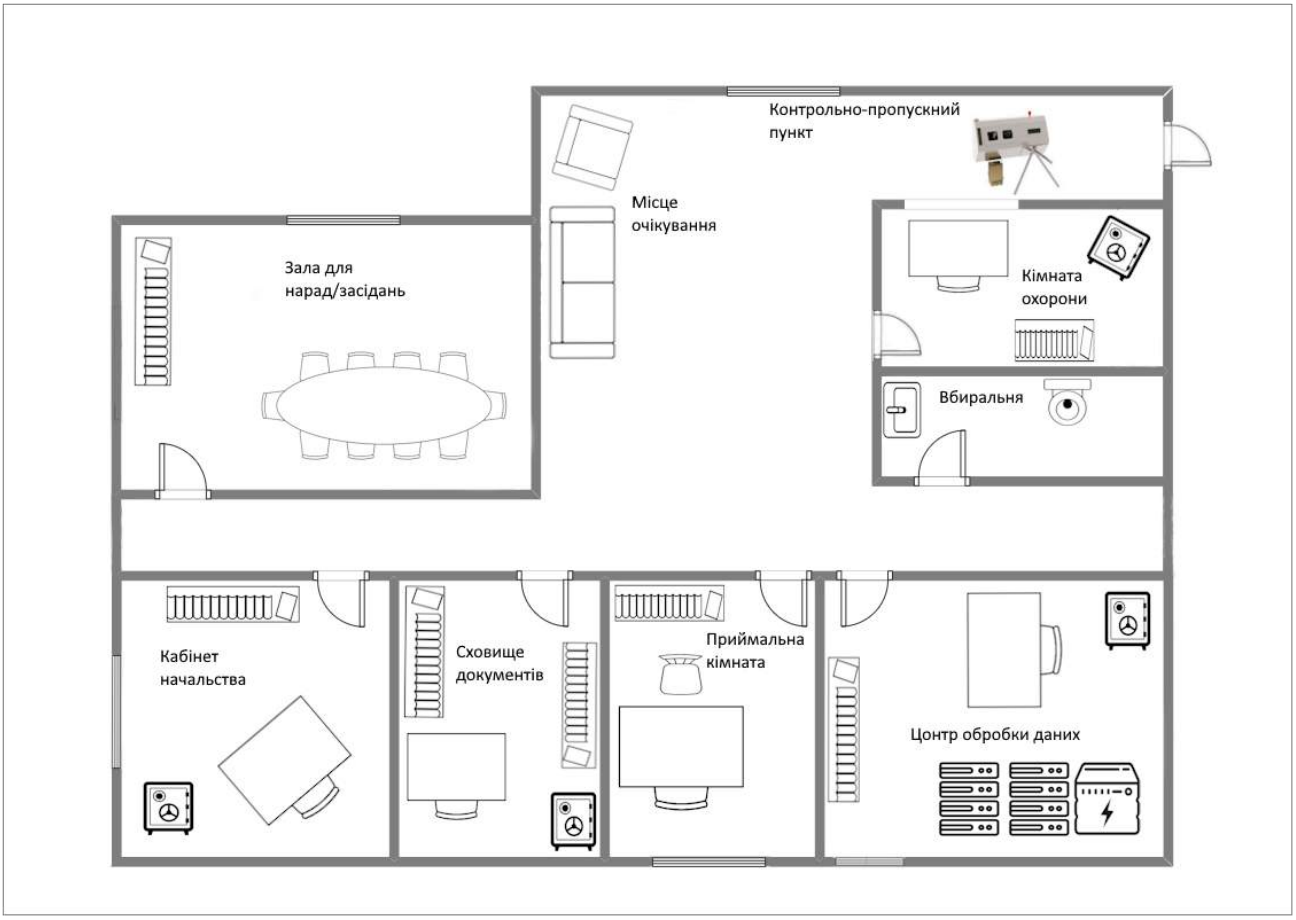
Для офісу компанії зазвичай потрібні такі основні кімнати:

- приймальня/зала очікування;
- кабінети для керівництва;
- кімната для нарад/переговорів;
- архів/сховище документації;
- серверна/технічна кімната;
- вбиральня.

Перейдемо до нашого плану який зображено на рисунку 3.8:

Центральна частина з ліва займає велика зала для нарад чи засідань. Поруч розташоване місце для очікування відвідувачів біля проходу через контрольно-пропускний пункт.

У правій частині є кімната охорони та вбиральня для персоналу чи відвідувачів. Нижній лівий сектор відведений під кабінет начальства та сховище документів.



3.8 – Схематичний план

У центрі нижньої частини знаходиться приймальна кімната для відвідувачів. В правому нижньому куті розміщено центр обробки даних. У плані передбачені проходи та коридори між зонами для зручного пересування. Загалом, цей функціональний план охоплює основні зони офісу.

Почнемо з зали для нарад/засідань, ця кімната призначення для проведення нарад. В цій кімнаті функціонує інформація в основному про порядок проведення роботи стосовно об’єкта і його особливостей.

На рисунку 3.9 зображено план зали нарад/засідань:

Вхідні двері:

- встановлено з двійним тамбуром;
- відчиняються через контролер доступу;
- вбудований датчик відкриття/закриття дверей.

Вікно:

- прикріплено два ВІ-3;
- використання щільних штор;
- використання датчика відкриття/закриття вікна.

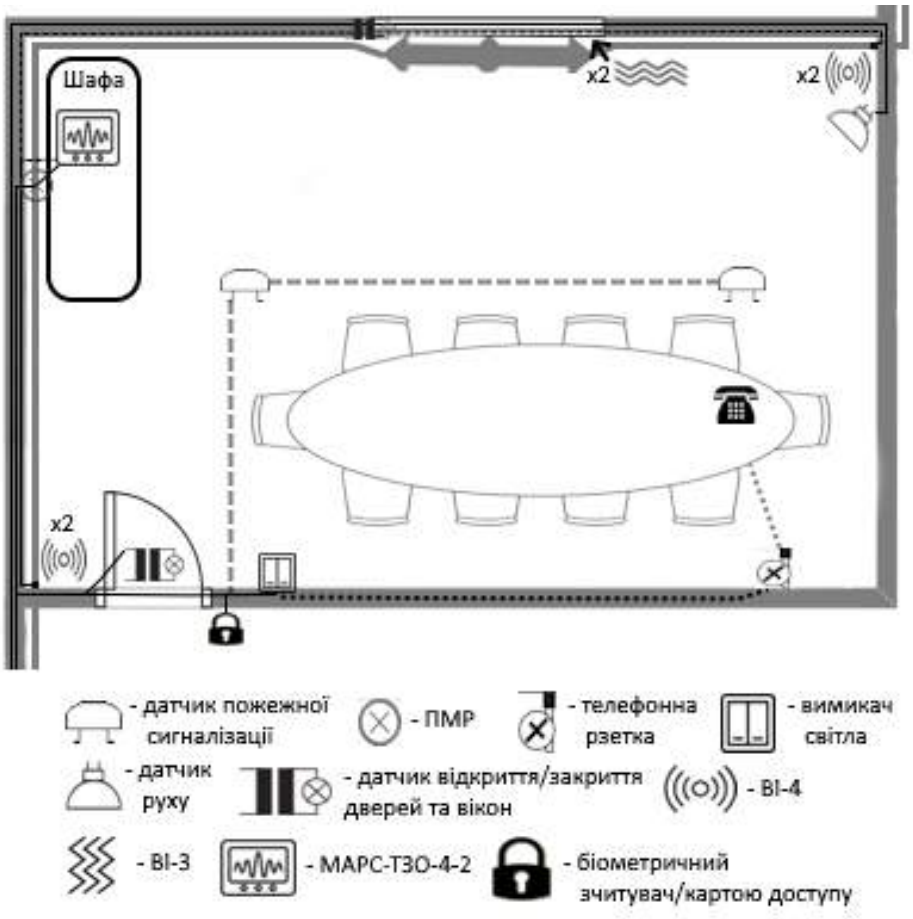


Рисунок 3.9 – Зала для нарад/засідань

Труби:

- у верхній правій частині два ВІ-4;
- у нижній лівій частині два ВІ-4.

Двійний тамбур, контролер доступу та датчик дверей захищають від несанкціонованого проникнення через вхід. Вібраційні датчики на вікнах та трубах. Датчик руху допомагає виявити присутність у приміщенні який розміщено в правому верхньому кутку на плані. Приховування МАРС у шафі робить систему безпеки менш помітною, за шафою реалізовано ПМР. Також встановлено два датчика пожежної сигналізації.

На рисунку 3.10 зображено кабінет керівництва фірми.

Вхідні двері:

- встановлено з двійним тамбуром;
- відчиняються через контролер доступу;
- вбудований датчик відкриття/закриття дверей.

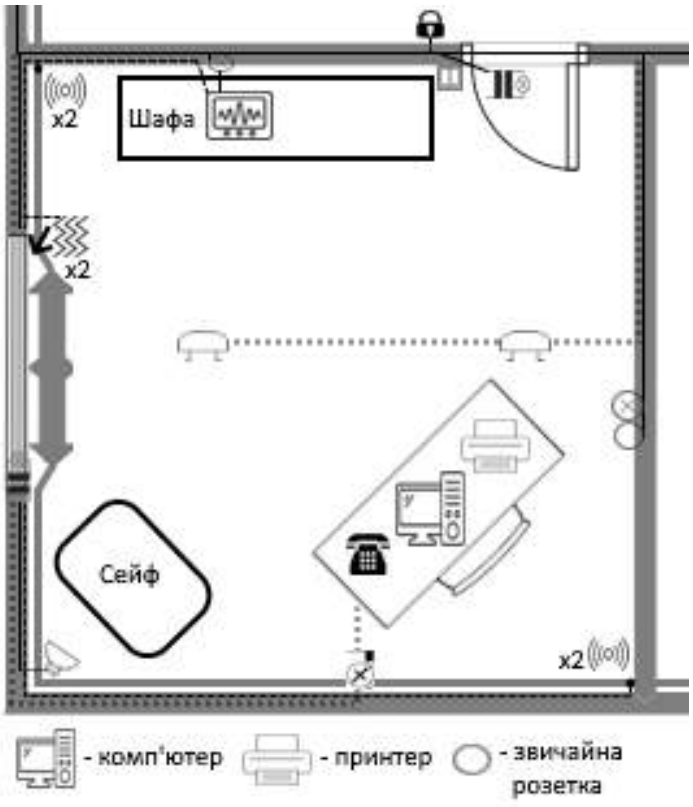


Рисунок 3.10 – Кабінет керівництва

Вікно:

- прикріплено два ВІ–3;
- використання щільних штор;
- використання датчика відкриття/закриття вікна.

Труби:

- у верхній лівій частині два ВІ-4;
- у нижній правій частині два ВІ-4.

У верхній частині розміщена шафа як і в попередній кімнаті в шафі приховано МАРС і за шафою і біля столу реалізовано ПМР. В лівому нижньому кутку розміщено датчик руху. Встановлено два датчики пожежної сигналізації.

На рисунку 3.11 зображено план сховища документів і приймальної кімната:

Сховище документів обладнано:

Вхідні двері:

- встановлено з двійним тамбуром;
- відчиняються через контролер доступу;
- вбудований датчик відкриття/закриття дверей.

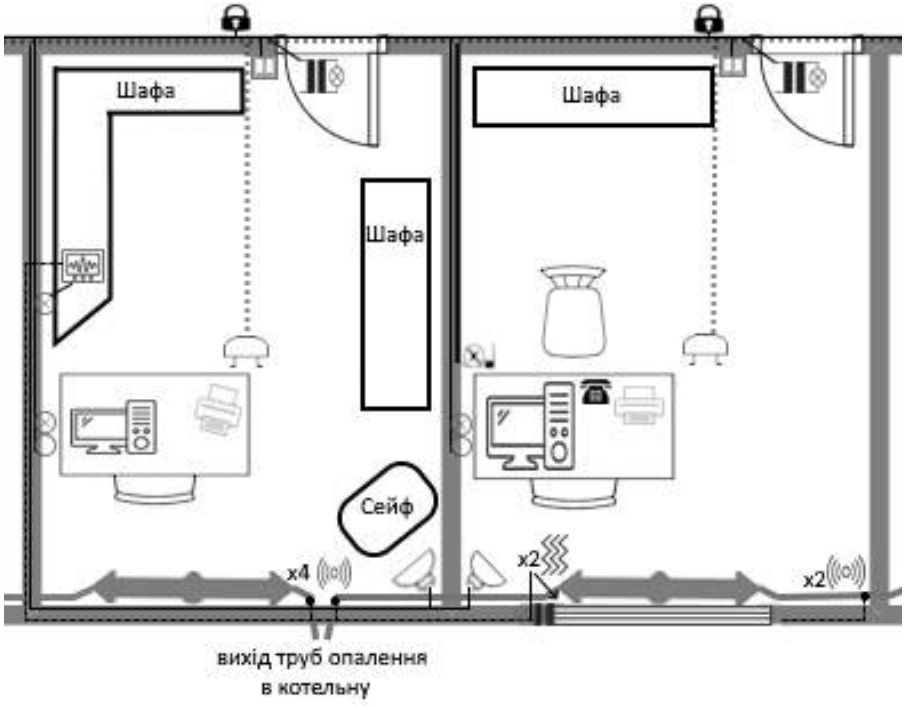


Рисунок 3.11 – Сховище документів і приймальна кімната

В верхньому лівому кутку розміщена шафа, в ній також прихований МАРС, за шафою біля розташування МАРС-а реалізований ПМР. Біля робочого столу також реалізовано ПМР і звичайно розетку. В нижній чистині вихід труб опалення до котельні і при виходах при стіні на трубах прикріплено ВІ-4. В правій нижній частині кімнати розміщено датчик руху і по середині датчик пожежної сигналізації.

Приймальна кімната:

Вхідні двері:

– встановлено з двійним тамбуром;

– відчиняються через контролер доступу;

– вбудований датчик відкриття/закриття дверей.

Вікно:

– прикріплено два ВІ-3;

– використання щільних штор;

– використання датчика відкриття/закриття вікна.

В нижньому лівому кутку розміщено датчик руху і по середині датчик пожежної сигналізації. В правій нижній частині прикріплено на труби два ВІ-4. Біля робочого столу встановлено звичайно розетку і реалізовано ПМР.

План центру обробки даних зображено на рисунку 3.12.

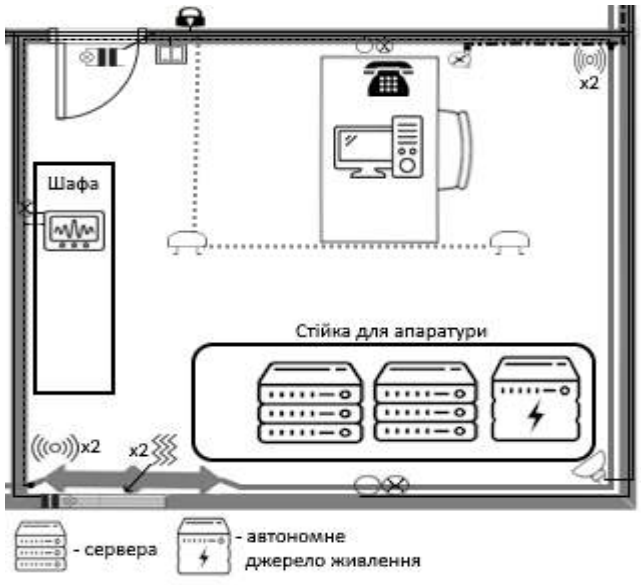


Рисунок 3.12 – Центр обробки даних

Вхідні двері:

– встановлено з двійним тамбуром;

– відчиняються через контролер доступу;

– вбудований датчик відкриття/закриття дверей.

Вікно:

– прикріплено два ВІ-3;

– використання щільних штор;

– використання датчика відкриття/закриття вікна.

Труби:

– у верхній правій частині два ВІ-4;

– у нижній лівій частині два ВІ-4.

В лівій частині розміщена шафа, в якій приховано МАРС, заді шафи реалізовано ПМР. У нижній частині в правому кутку розміщено датчик руху і по середині два датчика пожежної сигналізації. Біля столу встановлено звичайну розетку і реалізовано ПМР. Також на стойці для апаратури реалізовано автономне джерело живлення яке забезпечить живлення офісу при вимкненні світла.

На рисунку 3.13 зображено план кімнати охорони та вбиральні.

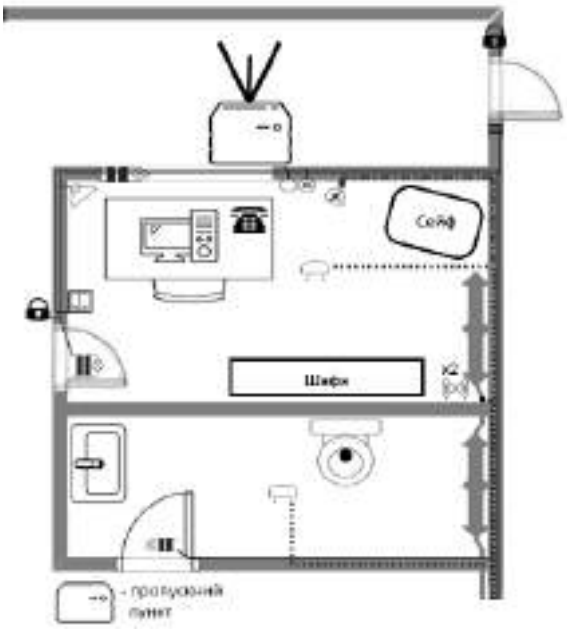


Рисунок 3.13 – Кімната охорони і вбиральня

Вбиральня:

На двері вбудовано датчик відкриття/закриття дверей. По центрі кімнати встановлено датчик пожежної сигналізації.

Кімната охорони:

Вхідні двері:

– встановлено з двійним тамбуром;

– відчиняються через контролер доступу;

– вбудований датчик відкриття/закриття дверей.

В верхньому лівому кутку встановлено датчик руху, по центрі встановлено датчик пожежної сигналізації. На вікні встановлено датчик відкриття/закриття. Біля столу встановлено звичайну розетку і реалізовано ПМР. В нижньому правому куті встановлено два ВІ-4.

На рисунку 3.14 наведено пдан-схему оснащення засобами захисту коридору і зони очікування.

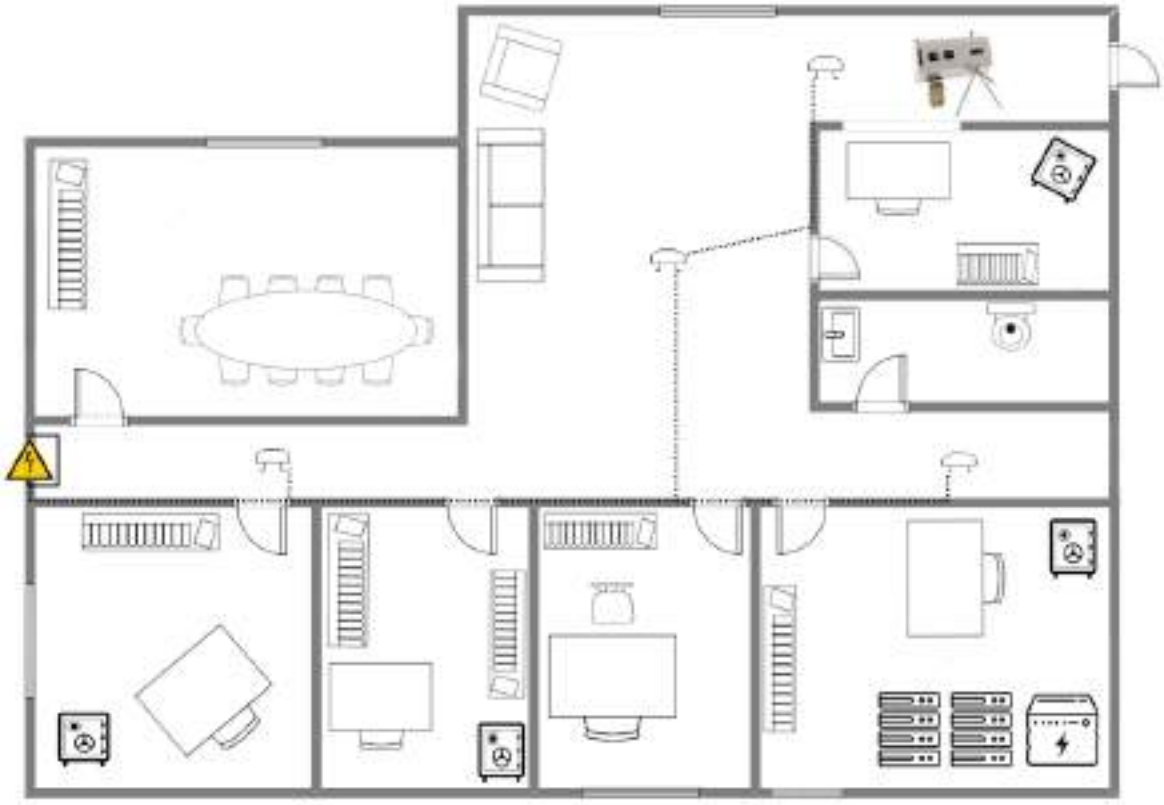


Рисунок 3.14 – Коридор і зона очікування

Двері входу в офіс також обладнані датчиком відкриття/закриття дверей і відчиняються через контролер доступу.

Також на рисунку 3.14 зображено розміщення датчиків пожежної сигналізації по коридору і зоні очікування.

3.5 Важливість обізнаності персоналу

Для компанії, яка спеціалізується на захисті інформації від витоку технічними каналами зв'язку, підвищення обізнаності персоналу про загрози інформаційній безпеці та методи їх запобігання є вкрай важливим з кількох ключових причин:

– людський фактор;

– постійний розвитку кіберзагроз;

– внутрішні політики та процедури безпеки;

– відповідальність і репутація компанії.

Людський фактор – є однією з найбільших загроз інформаційній безпеці. Необізнаний або недбалий персонал може стати вразливою ланкою, яка може призвести до витоку даних або проникнення зловмисників у системи компанії.

Постійний розвиток кіберзагроз – злочинці постійно вдосконалюють свої методи атак та соціальної інженерії. Співробітники повинні бути в курсі нових видів загроз і способів їх запобігання.

Внутрішні політики та процедури безпеки – співробітники повинні чітко розуміти і дотримуватися внутрішніх політик, стандартів і процедур компанії щодо інформаційної безпеки.

Відповідальність і репутація компанії як експерти в галузі інформаційної безпеки, компанія повинна демонструвати високі стандарти безпеки на власному прикладі функціонування.

Регулярні тренінги, орієнтація нових співробітників, періодичні нагадування, практичні вправи та тести допоможуть підвищити обізнаність персоналу та зміцнити культуру інформаційної безпеки в компанії.

Діаграма на рисунку 3.15 ілюструє важливість підвищення обізнаності персоналу щодо загроз безпеки інформації в компанії.

Рисунок 3.15 – Діаграма складової частини для підвищення обізнаності

Центральним елементом діаграми є «Підвищення обізнаності персоналу». Від нього відходять чотири гілки, що представляють ключові причини важливості цього заходу. Ця діаграма в простій візуальній формі демонструє, чому навчання та підвищення рівня обізнаності персоналу є критично важливим для забезпечення належного рівня інформаційної безпеки в компанії. зображено діаграму.

3.6 Висновок

У даному розділі нами було проведено дослідження компанії «SecurLine», яка спеціалізується на створенні систем захисту від витоку інформації технічними каналами зв'язку для державних інформаційних об'єктів ОІД. Було описано сферу діяльності компанії, перелік послуг, які вона надає, та категорії клієнтів.

При будівництві офісу компанії були реалізовані пасивні заходи захисту. Для активного захисту інформації в офісі були застосовані різноманітні засоби, такі як вібровипромінювачі ВІ-3 та ВІ-4, генератор шумових сигналів «МАРС-ТЗО-4-2», мережевий розв'язуючий пристрій «ПМР», датчики руху та розбиття скла Ajax CombiProtect Fibra, магнітоконтактні датчики Ajax DoorProtect Fibra та біометричний контролер доступу ZK Software MA300.

Представлено схематичний план офісу компанії з детальним описом розміщення та обладнання кожної кімнати, включаючи залу для нарад, кабінет начальства, сховище документів, приймальню, центр обробки даних, кімнату охорони та вбиральню. На планах позначено розташування датчиків, контролерів доступу, вібровипромінювачів та інших засобів захисту.

Наголошено на важливості підвищення обізнаності персоналу щодо загроз інформаційній безпеці та методів їх запобігання. Людський фактор, постійний розвиток кіберзагроз, дотримання внутрішніх політик безпеки та відповідальність і репутація компанії є ключовими причинами необхідності регулярного навчання та підвищення рівня обізнаності персоналу.

ВИСНОВКИ

У даній кваліфікаційній роботі було розроблено систему захисту офісу фірми від витоку інформації технічними каналами зв'язку. В ході дослідження було встановлено, що забезпечення надійного захисту конфіденційних даних є критично важливим для підтримки конкурентоспроможності та репутації компанії. Аналіз потенційних загроз і каналів витоку інформації показав необхідність реалізації комплексного підходу до безпеки, який включає як технічні, так і організаційні заходи.

При проектуванні системи захисту офісу фірми було враховано різноманітні технічні канали витоку інформації. Для протидії цим загрозам було запропоновано низку пасивних та активних заходів безпеки.

Особливу увагу було приділено плануванню та зонуванню офісного простору з метою мінімізації ризиків витоку інформації. Розроблений план офісу враховує розміщення чутливих зон, а також передбачає використання систем контролю доступу для запобігання несанкціонованому проникненню. Крім того, в роботі наголошується на важливості людського фактору в забезпеченні інформаційної безпеки.

Однак, слід пам'ятати, що забезпечення інформаційної безпеки є безперервним процесом, який вимагає постійного моніторингу, оновлення та адаптації до нових викликів і технологій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Бурачок Р. А., Климаш М. М., Коваль Б. В. Телекомунікаційні системи передавання інформації. Методи кодування: навч. посіб. Львів : політехніки, 2015. 476 с.

2. Інформаційна система та програмне забезпечення інформаційної. URL: http://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/95/95.html (дата звернення:24.02.2024).

3. Про захист інформації в інформаційно-комунікаційних системах. Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення 26.02.2024).

4. Кібербезпека та захист інформації. – URL: http://tr.knute.edu.ua/files/2021/05.pdf (дата звернення 28.02.2024).

5. Сащук Г. М. Інформаційна безпека в системі забезпечення національної безпеки. 2014. № 1. С. 46─50.

6. Коваленко, Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2010. № 3. с. 123–129.

7. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник: навч. посіб. Київ: ООО «Д.В.К.», 2004. 508 с.

8. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – Київ : «МК-Прес», 2005. 432 с.

9. Цілі інформаційної безпеки та їх значення. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yih-znachennya (дата звернення 12.03.2024).

10. Інформаційна безпека : навч. посіб. / В. В. Остроухов та інші 3-тє: вид. Ліра-К : 2021. 412 с.

11. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. No 2 (18). С. 16-22 (дата звернення 14.03.2024).

12. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок : Затверджено

наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 року №25. URL: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-tr-pemvn-95.pdf (дата звернення 22.03.2024).

13. Брагін А.С., Вульпе О.А. Передавальні та приймальні пристрої систем радіозв'язку : навч. посіб. ІВЦ «Політехніка» 2009, 130с.

14. Організаційне забезпечення захисту інформації : навч. посіб. / Лахно В.А., ті ін. 3-тє Київ : НУБіП України, 2022. – 432 с.

15. Л.С.Глоба. Математичні основи побудови інформаційно телекомунікаційних систем для студентів спеціальності 8.092401 «Телекомунікаційні системи та мережі» : навч. посіб. Київ : НТУУ «КПИ», 2006. 356 с.

16. Лебедєв О.М., Ладик О.І. Цифрова техніка: навч. посіб. Київ : Політехніка, 2004. – 320 с.

17. Чумаков В. І., Таранчук А. А., Харченко О. І. Моделювання пристроїв радіоавтоматики в системі MathCAD : навч. посіб. Хмельницький : ХНУ, 2011. 151 с.

18. Теорія радіолокаційних систем : навч. посіб. / Б. Ф. Бондаренко та ін. Київ : Видавничо-поліграфічний центр "Київський університет", 2008. - 359 с.

19. ДСТУ 7448:2013. Інформація та документація. Бібліотечно-інформаційна діяльність. Терміни та визначення понять. Чинний від 29.09.2013. Вид. офіц. Київ : УкрНДНЦ, 2014. 45 с.

20. Куйбіди В. С., Карпенка О. В. Інформаційно-комунікативна діяльність органів публічної влади : монографія. Київ : НАДУ, 2019. 358 с.

21. Коваленко А.Є. Побудова кодів на основі типових алгоритмів кодування даних : методичні вказівки із самостійної роботи студентів з дисципліни «Теорія інформації і кодування» : курс лекцій. Київ : ННК «ІПСА» НТУУ «КПІ», 2012. 71 с.

22. Згуровський М.З., Коваленко І.І., Міхайленко В.М. Вступ до комп‘ютерних інформаційних технологій: навч. посіб. Київ : Вид-во Європ. ун-ту, 2000.- 265 с.

23. Банкет В.Л. Заводостійке кодування в телекомунікаційних системах : навч. посіб. Одеса : ОНАЗ ім. О. С. Попова, 2011. 100 с.

24. Білинський Й.Й., Огородник К.В., Юкиш М.Ю. Електронні системи : навч. посіб. Вінниця : ВНТУ, 2011. 209с.

25. Artificial Intelligence’s Impact on the Restaurant Industry URL: https://modernrestaurantmanagement.com/artificialintelligences-impact-on-the-restaurant-industry/ (дата звернення 30.04.2024).

26. Kocher Paul. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Advances in Cryptology–CRYPTO’96 : journal. Vol. 1109. P. 104–113.

27. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.1999 р. No 1229. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення 04.05.2024).

28. Концепція технічного захисту інформації В Україні. Затверджено постановою Кабінету Міністрів України від 08.10.1997 року No 1126. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text (дата звернення 07.05.2024).

29. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту / Іванченко С.О. та ін. 3-тє. Київ : НТУУ «КПІ», 2016. 101 с.

30. Богданович, В.Ю., Бадрак В.В. Конкурента розвідка та промислове шпигунство. 2014. № 1. С. 16-22. URL: Режим доступу: http://nbuv.gov.ua/UJRN/szi_2014_1_5 (дата звернення 09.05.2024).

31. Лісовець С. М. Акустичний контроль матеріалів із неоднорідною структурою методами нелінійної акустики. Вісник Київського національного університету технологій та дизайну. Серія : Технічні науки. 2015. № 1. С. 110-116. URL: http://nbuv.gov.ua/UJRN/vknutdtn_2015_1_17 (дата звернення 10.05.2024).

32. Ніколаєнко, Ю. С. Протидія радіотехнічній розвідці. Системи безпеки, зв'язку та телекомунікацій. 1995. №6. С. 12 - 15. URL: http://nbuv.gov.ua/UJRN/efek_2015_11_53 (дата звернення 12.05.2024).

33. Гуржій А.М. Електротехніка та основи електроніки : навч. посіб. Київ : Літера ЛТД, 2020. 293с.

34. Пілінський В. В. Електромагнітна сумісність радіоелектронних засобів : курс лекцій. Київ : НТУУ «КПІ», 2008. 374 с.

35. Москаленко Н. О., Леонова Теоретичні Ю. О. Теоретичні підходи до конкурентної розвідки та особливості її аналітичного забезпечення. Проблеми економіки. 2018. № 2. С. 228-234. URL: http://nbuv.gov.ua/UJRN/Pekon_2018_2_32 (дата звернення 20.05.2024).

36. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи. Інформація і право. 2017. № 4. С. 62-72. URL: http://nbuv.gov.ua/UJRN/Infpr_2017_4_8 (дата звернення 21.05.2024).

37. Photonic approach for microwave spectral analysis based on Fourier cosine transform / Yun Wang, Hao Chi, Xianmin Zhang, Shilie Zheng, Xiaofeng Jin : Optics let. 2011. Vol. 36, № 19. P. 3897-3899.

38. Проблема електромагнітної сумісності електромеханічних систем. питання забезпечення надійної та безперебійної роботи. URL: https://org2.knuba.edu.ua/mod/book/tool/print/index.php?id=36013&chapterid=592 (дата звернення 23.05.2024).

39. Закладні пристрої. Способи їх застосування. URL: https://iac.com.ua/uk/news/napivprovidnikova-radiorevolyucziya-ta-ii-naslidki/ (дата звернення 24.05.2024).

40. Проведення спеціального обстеження об'єктів з метою виявлення закладних пристроїв. Джерела загроз інформаційної безпеки. URL: http://securepolicy.blogspot.com (дата звернення 24.05.2024).

41. Звукоізоляція міжповерхових перекриттів. URL: https://www.shumanet.ua/ua/albom_solutions/flats/zvukoizolyaciya_perekrytiy/. (дата звернення 26.05.2024).

42. Плаваюча підлога, технічне рішення. . – URL: https://shpalerkley.cx.ua/45-styazhka-z-pinoplastu-yak-zrobiti-pidlogu-z.html. (дата звернення 26.05.2024).

43. Методи та засоби захисту інформації. URL: http://www.bestreferat.ru/referat218628.html (дата звернення 28.05.2024).

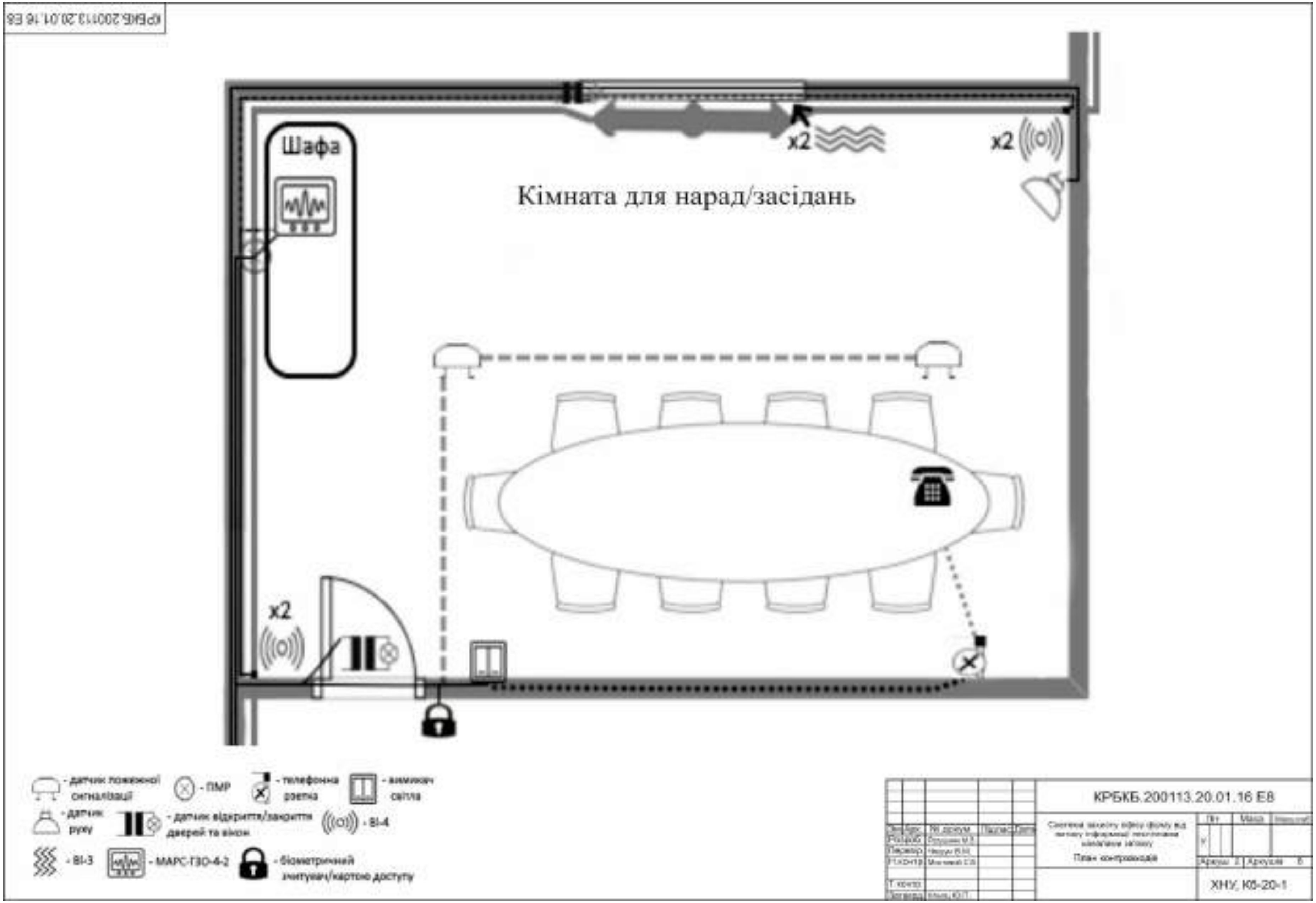
44. Технічний захист інформації. URL: https://tzi.com.ua/obladnannya.html (дата звернення 29.05.2024).

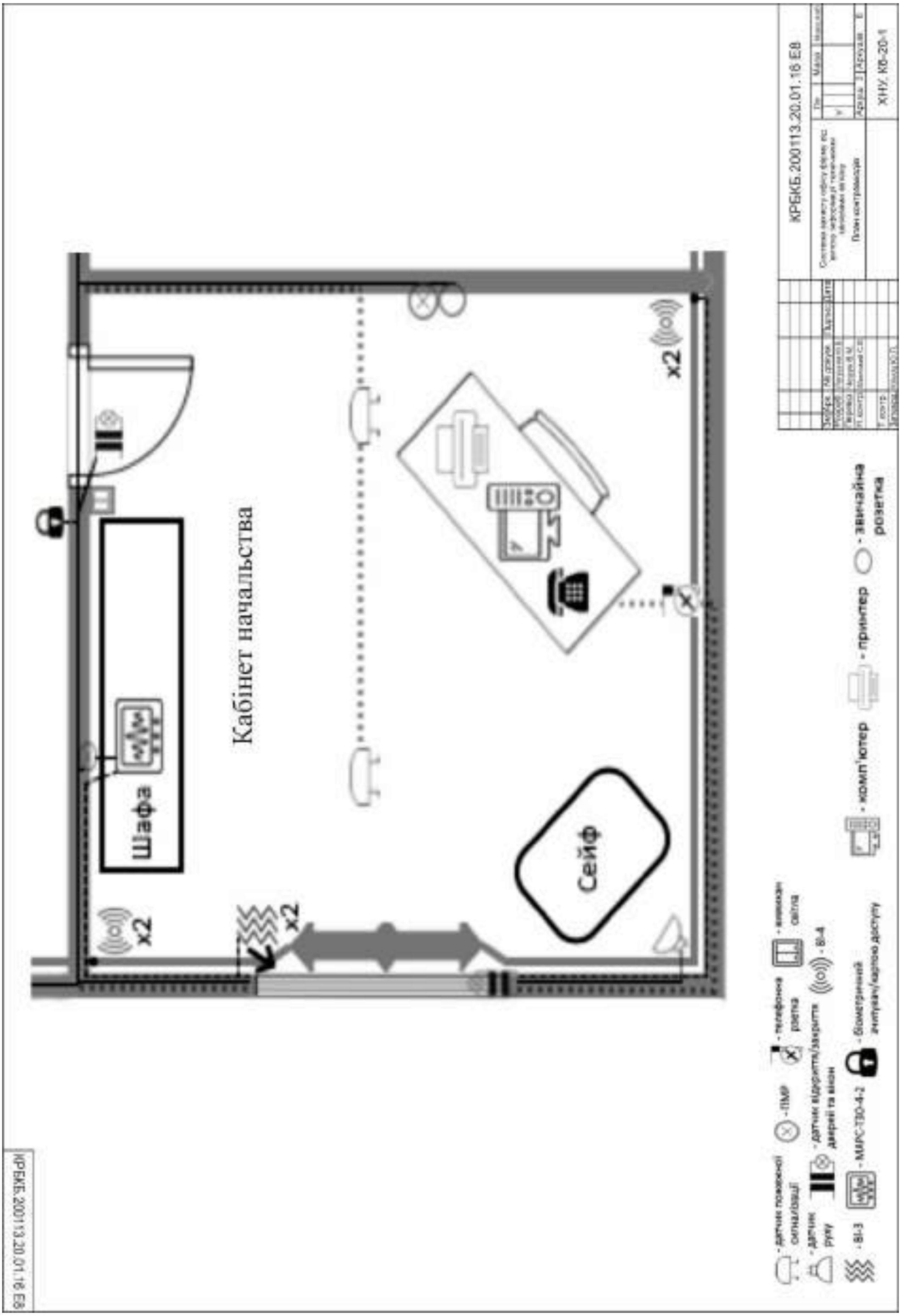
ДОДАТОК А

(Обов’язковий)

Копії графічної частина

Типи шпигунських пристроїв	Методи встановлення	Ці атаки	Можливі висліки	Заходи протидії
Аудіо жучки	Фізичний доступ до приміщення	Конфіденційна інформація	Фінансові втрати	Фізичний контроль доступу
Відеокамери	Соціальна інженерія	Компрометація таємниця	Підрив репутації	Технічні засоби захисту (блокування портів, шифрування)
Клавіатурні логери	Фішингові атаки	Особисті дані співробітників	Втрата конкурентних переваг	Політики безпеки та навчання співробітників
Перехоплювачі мережевого трафіку	Комбінація фізичного та програмного доступу	Комунікації керівництва	Компрометація особистих даних співробітників	Використання засобів виявлення шпигунських пристроїв (наприклад, RF-детектори).
GPS трекери	Прикріплення до транспортних засобів або обладнання	Локація та перемішення об'єктів	Порушення конфіденційності переміщень	Регулярні перевірки транспортних засобів та обладнання.
Знімні носії інформації (USB, SD-карти)	фізичний доступ до комп'ютерів та серверів	Копіювання даних	Витік критичної інформації	Заборона використання знімних носіїв.
Мобільні пристрої (телефони, планшети)	Використання соціальної інженерії та фішингу	Персональні та корпоративні дані	Компрометація конфіденційної інформації	Політики використання мобільних пристроїв.

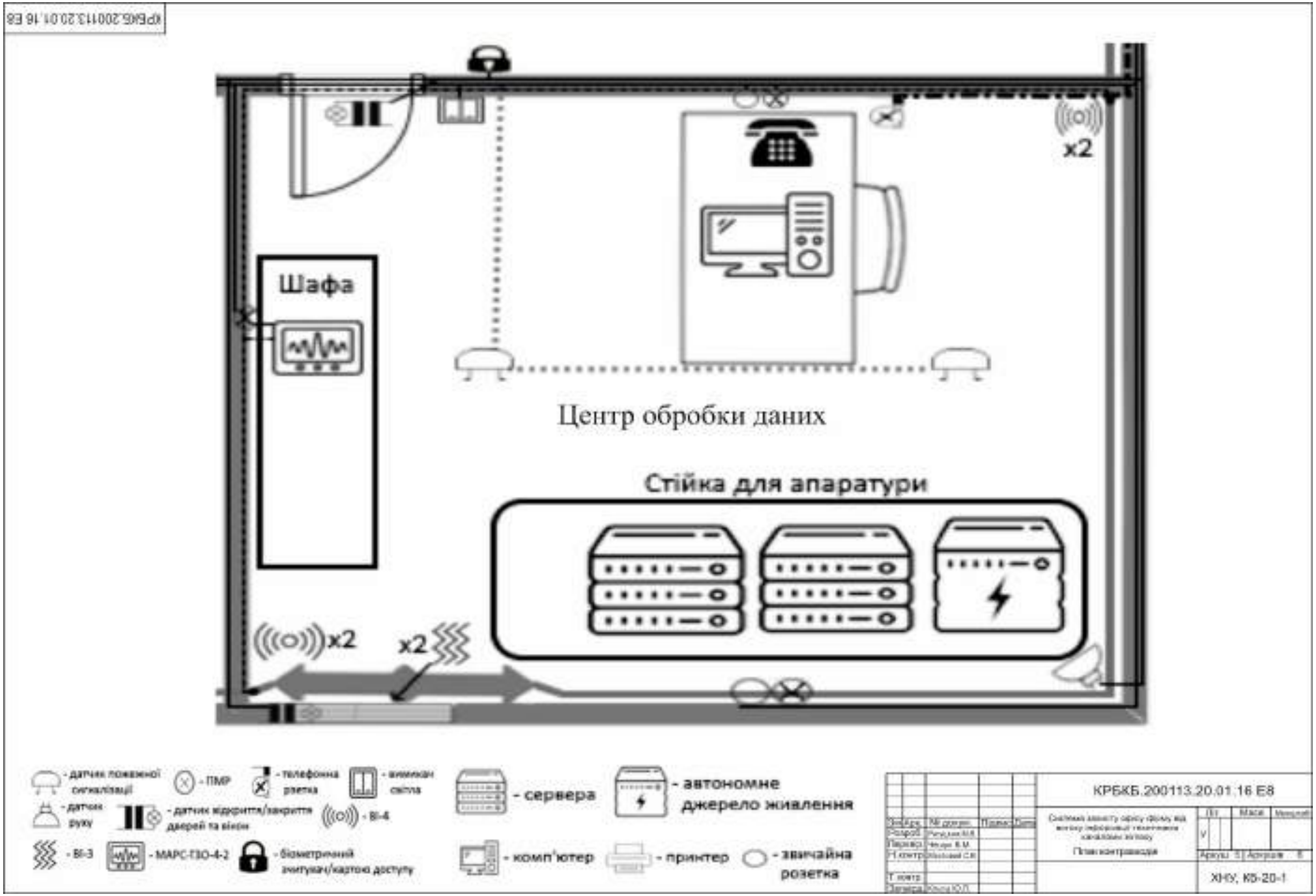

КРБКБ.200113.20.01.16 Е8
Шафа
x2
x2
Кімната для нарад/засідань
x2
- датчик пожежної сигналізації
- ПМР
- телефонна розетка
- вимикач світла
- датчик руху
- датчик відкриття/закриття дверей та вікон
- ВІ-4
- ВІ-3
- МАРС-ГЗО-4-2
- біометричний зчитувач/картою доступу
КРБКБ.200113.20.01.16 Е8
ХНУ, КБ-20-1


Кабінет начальства
Шафа
Сейф
x2
x2
x2
КРБКБ.200113.20.01.16 Е8
КРБКБ.200113.20.01.16 Е8
ХНУ, КБ-20-1
- датчик руху
- ПМР
- телефонна розетка
- ВІ-3
- ВІ-4
- МІРС-ТЗО-4-2
- біометричний зчитувач/картою доступу
- комп'ютер
- принтер
- звичайна розетка

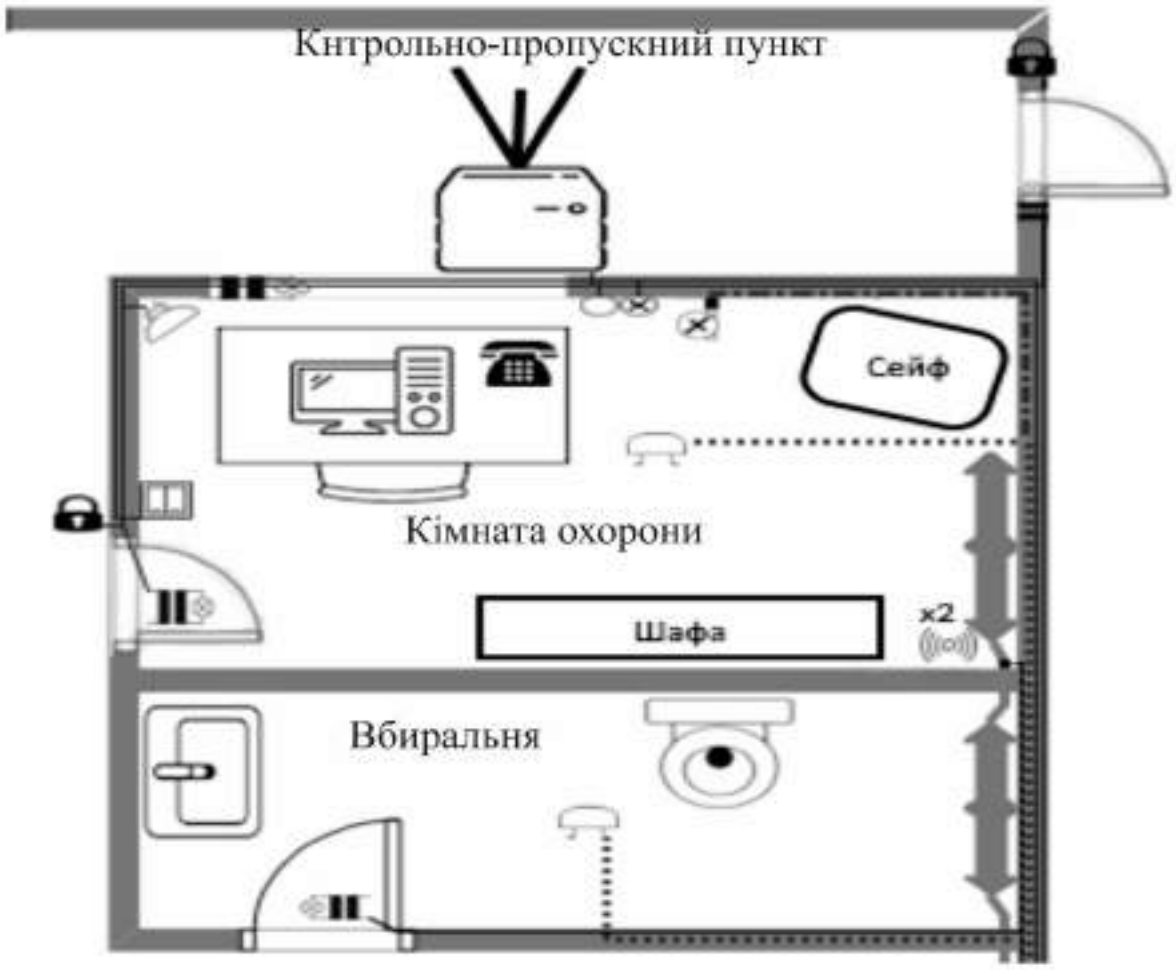
КРБКБ.200113.20.01.16 Е8

- датчик пожежної сигналізації
- ПМР
- телефонна розетка
- вимикач світла
- датчик руху
- датчик відкриття/закриття дверей та вікон
- ВІ-4
- ВІ-3
- МАРС-ТЗО-4-2
- біометричний зчитувач/картою доступу
- комп'ютер
- принтер
- звичайна розетка

Зм.	Арк.	№ докум.	Підпис	Дата	КРБКБ.200113.20.01.16 Е8		
Розроб.		Петрович М.О.			Система захисту офісу фірми від витоку інформації технічними каналами зв'язку	Літ.	Маса	Масштаб
Перевір.		Чернух В.М.			План контролю(а)			
Н.контр.		Мостовий С.В.				Аркуш 4	Аркушів 6	
Т.контр.						ХНУ, КБ-20-1		
Затверд.		Власів Ю.П.						


КРБКБ.200113.20.01.16 Е8
Шафа
x2
Центр обробки даних
Стійка для апаратури
- датчик пожежної сигналізації
- ПМР
- телефонна розетка
- вимикач світла
- датчик руху
- датчик відкриття/закриття дверей та вікон
- ВІ-4
- ВІ-3
- МАРС-ГЗО-4-2
- біометричний зчитувач/картою доступу
- сервера
- автономне джерело живлення
- комп'ютер
- принтер
- звичайна розетка
ХНУ, КБ-20-1

КРБКБ.200113.20.01.16 Е8



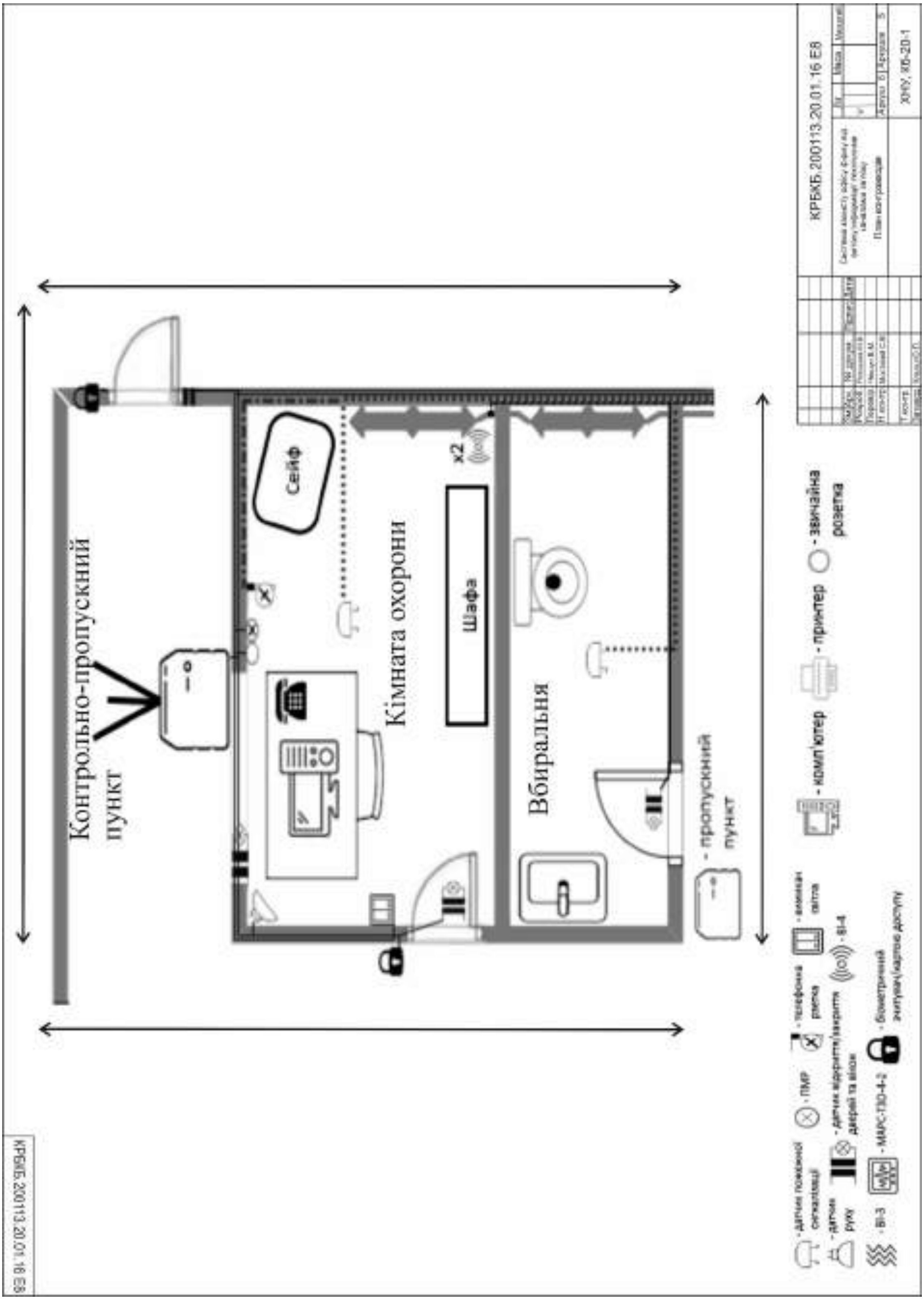
- датчик пожежної сигналізації
- ПМР
- телефонна розетка
- вимикач світла
- датчик руху
- датчик відкриття/закриття дверей та вікон
- Ві-4
- Ві-3
- МАРС-ТЗО-4-2
- біометричний зчитувач/картою доступу
- комп'ютер
- принтер
- звичайна розетка

КРБКБ.200113.20.01.16 Е8

Система захисту офісу фірми від витоку інформації технічними каналами зв'язку

План-контрольця

ХНУ, КБ-20-1


Контрольно-пропускний пункт
Кімната охорони
Вбиральня
Сейф
Шафа
x2
- пропускний пункт
- комп'ютер
- принтер
- звичайна розетка
КРБКБ.200113.20.01.16 Е8
ЗНУ, ЗІБ-20-1

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.

Ратушняка Максима Віталійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.06.24
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016376586

Дата перевірки:
19.06.2024 22:13:36 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
19.06.2024 22:58:10 EEST

ID користувача:
100008300

Назва документа: Ратушняк_Максим_Диплом плагіат

Кількість сторінок: 59 Кількість слів: 8515 Кількість символів: 72657 Розмір файлу: 1.28 MB ID файлу: 1016184693

3.68%
Схожість

Найбільша схожість: 0.8% з Інтернет-джерелом (https://nadzor.ua/uk/product/provodnoj-datcik-otkrytia-ajax-doorpro...

3.2% Джерела з Інтернету 265 ..... Сторінка 61

1.23% Джерела з бібліотеки 40 ..... Сторінка 62

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 1

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

ID: 131638 Назва: Система захисту офісу фірми від витоку інформації технічними каналами зв'язку Додано в БД: 2024-06-19 Автора: Ратушняк М.В. Керівники: Чешун В.М. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	57877	879	1097 (2%)	18 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту офісу фірми від витоку інформації технічними каналами зв'язку

Автор: Ратушняк Максим Віталійовича

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Керівник: Чешун Віктор Миколайович, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 96,32%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v 15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Ратушняк Максим Віталійович

Тема Система захисту офісу фірми від витоку інформації технічними каналами зв'язку

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 6 ; кількість сторінок записки 67 .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система захист офісу фірми «SecurLine».. Ця система передбачає захист інформації від витоку різними акустичними каналами зв'язку. У процесі виконання кваліфікаційної роботи було досліджено поняття захищеності, технічні канали зв'язку. Було проаналізовано можливі загрози для офісу компанії і на основі цих загроз розроблялась система захисту, ще було розроблено пасивні заходи захисту. Визначились і ознайомились з засобами захисту для побудови системи захисту. Також було побудовано схематичний план офісу і окремі плани контрзаходів для кожного з приміщень

2. Висновок про відповідність кваліфікаційної роботи завданню. У кваліфікаційній роботі успішно реалізовано завдання як у теоретичній, так і в практичній частинах, з дотриманням усіх встановлених вимог.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У кваліфікаційній роботі було виконано кілька завдань, зокрема у першому розділі дослідження поняття захищеності і системи захисту, та її складових. Опис системи захисту інформації та її компонентів. Досліджено технічні канали в системі і їх функціонування. Класифікація каналів витоку інформації. Опис функціонування різних типів каналів витоку. Визначення технічних каналів витоку інформації. Було перелічено та описано різні види технічних каналів. Постановлені проблеми захисту інформації від витоків. Визначення цілей та завдань дослідження. У другому розділі після постановки завдань було проаналізовано можливих ризиків і загроз і класифікація та опис різних видів ризиків і загроз. Визначено і описано заходи запобіганню витоку інформації. В третьому розділі було аналізовано специфіки діяльності та інформаційних ресурсів, проведено пасивні заходи захисту офісу. Впроваджено засоби захисту в систему захисту. Планування офісу і системи захисту в ньому, реалізація комплексу заходів захисту. Окрім того було виділено Роль людського фактору в забезпеченні інформаційної безпеки.

4. Позитивні сторони роботи Розроблена система захисту офісу фірми від витоку інформації технічними каналами зв'язку є акутальною, має практичну цінність і є орієнтованою на конкретну фірму-замовника.

5. Негативні сторони роботи В роботі відсутній огляд існуючих рішень систем-аналогів і аналіз їх недоліків та переваг. В самому проєкті недостатня увага приділена дослідженню обладнання і офісної техніки, що використовується співробітниками фірми, та загрозам витоку інформації електромагнітними каналами з урахуванням властивостей цього обладнання

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень у проєктуванні та супроводі розробленої комплексної системи захисту інформації.

8. Інші зауваження В роботі забагато уваги приділено опису технічних характеристик використаного обладнання для технічного захисту інформації.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є «добре»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мішан Віктор Володимирович
доцент кафедри ТМІТ, кандидат технічних наук

« 18 » 06 2024. (підпис)